APPENDIX E

SUPPORTING AUTOMATION EQUIPMENT WITHIN DIGITIZED ARMY

Introduction

This appendix describes the tactics, techniques and procedures required for supporting automation equipment within the digitized Army. It provides information on the mission, functions, and organizations providing automation support and is directed towards the commanders and staff. The special text outlines the functions and operations of each support element supporting Division automation. This includes hardware, software, and network support responsibilities.

This appendix also integrates varied maintenance plans into a support concept that applies only to the support of stand-alone computer systems. It does not apply to automation embedded within weapon systems and platforms. Although this appendix targets the digitized Army, the procedures described can be applied to all types of Army organizations.

Note: This ST does not attempt to list all Army Battle Command Systems (ABCS), Standard Army Management Information Systems (STAMIS), Combat Support Systems (CSS), Support Automation, and Network Devices or functions associated with digitizing the Army. System and Network Administration procedures and responsibilities may be found in the following Signal Doctrinal Manuals: FM 6-02.7 **(FM 24-7),** ***Tactical Local Area Network (LAN) Management Techniques*****,** FM 6-02.32 **(FM 11-32),** ***Combat Net Radio Operations,*** FM 6-02.41 **(FM 24-41),** ***Tactics, Techniques and Procedures (TTP) for Enhanced Position Location Reporting System (EPLRS),*** FM 6-02.71 **(FM 11-71),** ***Network and Systems Management,*** FM 6-02.42 **(FM 11-41),** ***Signal Support - Echelons Corps and Below,*** FM 6-02.50 **(FM 11-50),** ***Combat Communications (Hvy&Lht) Divisions, and*** FM 6-02.69 **(FM 24-69),** ***Signal Digital Equipment Procedural Guide.***

Supporting Automation

The revolution in military operations is rapidly transforming the Army into a highly lethal, technologically advanced fighting force. This transformation to a digital, information-based Army requires a substantial investment in automation and network communication equipment. Thousands of computers are currently being developed, tested, and fielded to provide commanders and leaders at every level near-real-time situational awareness on the battlefield. This chapter provides a brief description of the supported automation equipment.

AUTOMATION EQUIPMENT

The digitized Army will employ a wide variety of automation equipment ranging from simple commercial-off-the-shelf (COTS) laptop computers to ruggedized

UNIX-based command and control (C2) systems. This publication recognizes that support for these systems varies and attempts to categorize the equipment accordingly. Automation equipment can essentially be categorized into three distinct types: the Army Battle Command and Control System (ABCS), the Standard Army Management Information System (STAMIS), and Support Automation.

Army Battle Command Systems (ABCS)

ABCS consists of the various C2 systems aimed at enabling commanders to "see and understand" the battlespace. ABCS is a system of systems designed to assist commanders in exercising C2 of available forces in mission accomplishment. ABCS is the integration of fielded, developmental, and future automated information systems (AISs) employed in both training and tactical environments.

Note: A description of ABCS is covered in Appendix A or FM 24-7.

Standard Army Management Information Systems (STAMIS)

The combat service support (CSS) community has developed functional information management systems that increase the productivity of the individual soldier and effectiveness of the unit. These systems provide the infrastructure required for any military ground operation. The technical goal is to establish a seamless and interoperable network. The network involves the integration and communication software used by all STAMIS systems which include–

- Unit-Level Logistics System-Aviation (ULLS-A)
- Unit Level Logistics System-Ground (ULLS-G).
- Unit Level Logistics System-S4 (ULLS-S4).
- Standard Property Book System-Redesign (SPBS-R).
- Standard Army Retail Supply System (SARSS-1 and SARSS-2AD).
- Standard Army Maintenance System (SAMS-1 and SAMS-2).
- Standard Installation/Division Personnel System-3 (SIDPERS-3).
- Department of the Army Movement Management System-Redesign (DAMMS-R).
- Standard Army Ammunition System-Modernization (SAAS-Mod).
- Theater Army Medical Management Information System (TAMMIS)
- Medical Communications for Combat Casualty Care (MC4)

Note: Descriptions of the above systems are listed in Appendix A.

STAMIS systems are Commercial off-the-Shelf (COTS) computers with evolving open-system software to enhance sustainment capabilities. An important tenet of this architecture is that a division or separate brigade will use nothing larger than a desktop personal computer (PC). Each unit's computer is equipped with software to support critical functions from the motor pool to the battalion aid station. STAMIS provides automated support/information for the following CSS functions:

- Supply/property accountability.
- Medical logistics.
- Maintenance.
- Transportation.

- Personnel.
- Financial management.
- Ammunition.
- Command and Control (C2) (Combat Service Support Control System (CSSCS)).
- Personnel service support (legal, chaplain, finance, postal services, and so forth).

Note: The hardware of nonlogistical personnel service support systems (Legal, Chaplain, Finance, Postal Services, e.) are not supported by STAMIS. COTS or Support Automation hardware platforms are used to support these types of management systems. These application services are not listed under support automation, but the hardware support for these nonlogistical items are explained.

SUPPORT AUTOMATION

Support automation includes COTS, government-off-the-shelf (GOTS), and automated data processing equipment (ADPE) systems. These systems (less ABCS and STAMIS) are necessary for a unit to accomplish its assigned mission. Some examples of COTS equipment include desktop Personnel Computers (PCs), laptop computers, compact disk-read only memory (CD-ROM) readers, and peripheral devices. Table(s) of organization and equipment (TOE), tables of distribution and allowances (TDA), common table of allowances (CTA) 50-909, or appropriate major Army command (MACOM) directorate may authorize this equipment.
COTS equipment is normally acquired with manufacturers warranties. However, these warranties are frequently voided and impractical for units in a deployed environment.

NETWORK DEVICES

Network devices are digital devices and peripherals that support the inter/intra connection of data/voice/video communications. This broad range of devices encompasses all network devices necessary to make up the local area network (LAN) and wide area network (WAN). Some examples of network devices include inline network encryption (INE) devices, routers, hubs, and switches.

Staff Roles and Responsibilities

INTRODUCTION

The management and support of automation poses numerous challenges for Army leaders. This section identifies the roles and responsibilities of key personnel within Corps, Divisions, and Support Commands. It focuses on those tasks and responsibilities associated with the planning, management, operation and support of automation. Except where noted, the commanders and staff leaders listed below are authorized at every level from battalion to corps. FM 101-5 provides additional information on staff responsibilities and duties.

Today's Automated Information Systems (AIS) are extremely complex and require support from various sources to ensure their successful operation. The Army currently trains selected military occupational specialties to troubleshoot computer hardware, networking equipment, and operating systems. This training seldom includes troubleshooting of the multitude of software applications resident on Army AIS. The actual users of the AIS are the best trained to provide the system specific application support.

This publication designates staff responsibility for various ABCS and STAMIS systems to facilitate application training and support. While the G6/S6 is responsible for the overall health of all AIS within the unit, other staff sections and organizations are required to provide the necessary system specific application support.

COMMANDER

The commander provides purpose and direction to soldiers. He positions himself on the battlefield where he can best facilitate accomplishing the mission. He is responsible for:

- Establishing automation support priorities
- Ensuring subordinate leaders are trained in the employment, operation and sustainment of automation
- Providing command and control of automation resources

CHIEF OF STAFF/EXECUTIVE OFFICER

There is a Chief of Staff (CofS) at Corps and Division and an Executive Officer (XO) at brigade and battalion. The CofS/XO is the commander's principal assistant for directing, coordinating, supervising, and training the staff. The commander normally delegates executive management authority to the CofS/XO. They are responsible for directing the execution of staff activities. They exercise overall responsibility by:

- Providing command guidance for automation support
- Coordinating the staff to ensure ABCS integration
- Coordinating the staff to ensure automation support
- Managing the Commander's Critical Information Requirements (CCIR)
- Directly supervising the main command post (CP) and headquarters cell to include displacement, protection, security, and communications
- Ensuring the staff integrates and coordinates its activities internally, vertically (with higher headquarters and subordinate units), and horizontally (with adjacent units)

PRIMARY STAFF

Primary staff officers are the commander's principal staff assistants and are directly accountable to the XO/CofS. The staff helps the commander coordinate and supervise the execution of plans, operations, and activities. The staff processes and analyzes information and makes recommendations to assist the commander in decision-making.

G1/S1

The G1/S1 is the principal staff officer for all matters concerning human resources (military and civilian) that include personnel readiness, personnel services, and administrative headquarters management. As the staff proponent for SIDPERS, the G1/S1is also responsible for:

- Supervising SIDPERS operations and support
- Providing guidance on the employment and support of SIDPERS
- Providing software application expertise for SIDPERS
- Coordinate with the G-4 to insure that the CSSCS network supports personnel operations.

G2/S2

The G2/S2 is the principal staff officer for all matters concerning military intelligence, counterintelligence, security operations, and military intelligence training. Specific responsibilities include seven major tasks: direct, collect, analyze, disseminate, present enemy information, assist in attacking enemy C2, and assist in protecting friendly C2. As the staff proponent for ASAS-RWS and IMETS, the G2/S2 is also responsible for:

- Supervising All Source Analysis System-Remote Workstation (ASAS-RWS) and Integrated Meteorological System (IMETS) operations and support
- Providing guidance on employment and support of ASAS-RWS and IMETS
- Providing software application expertise for ASAS-RWS and IMETS
- Supervising the command security program and evaluate physical security vulnerabilities (See AR 190-13, AR 190-51, and AR 380-19)
- Assist the G6/S6 in implementing and enforcing LAN security policies

G3/S3

The G3/S3 is the principal staff officer for all matters concerning training, operations and plans, and force development and modernization. The G3/S3 is also responsible to the XO/CofS for integrating all ABCS systems and their use in supporting the tactical mission. The G3/S3 also serves as the staff proponent for Maneuver Control System (MCS), Advanced Field Artillery Tactical Data System (AFATDS), Air and Missile Defense Workstation (AMDWS), Forward Area Air Defense Command , Control, Computer and Intelligence System (FAADC3I), and Force XXI Battle Command-Brigade and Below (FBCB2). He accomplishes these responsibilities by:

- Planning, operating and employing ABCS
- Providing operational and support guidance to subordinate units
- Coordinating with the G6/S6 for communications connectivity for the system
- Providing software application expertise on proponent systems
- Monitors and reports the readiness of all ABCS systems

- Develop CONOP/restore/transition plans for integrated information operations
- Develop and execute sustainment training programs for battlefield automation

G4/S4

The G4/S4 is the principal staff officer for coordinating the logistical integration of supply, maintenance, transportation, and services. The G4/S4 is the link between the support unit and his commander plus the rest of the staff. The G4/S4 assists the support unit commander in maintaining logistics visibility with the commander and the staff. He must maintain close and continuous coordination with the G3/S3 and the support command commander who is responsible for support of tactical operations. The G4/S4 is the staff proponent for CSSCS/Logistical STAMIS. He is also responsible for:

- Coordinating maintenance support
- Coordinating all classes of supply (less VIII)
- Coordinating the requisition, acquisition, and storage of supplies and equipment and the maintenance of materiel records
- Supervising CSSCS operations and support
- Providing guidance on employment and support of CSSCS
- Monitoring and reporting the status of all automation equipment
- Planning, integrating, and employing logistical STAMIS
- Coordinate all internet dependent STAMIS actions with G6
- Providing software application expertise on CSSCS
- Establishing and enforcing CSSCS operational standards.

G6/S6

The G6/S6 is the principal staff officer for all matters concerning signal operations, automation management, network management, and information security. The G6/S6 coordinates communications requirements to support missions and prepares appropriate plans and orders. As the network administrator, the G6/S6 installs and maintains the transport infrastructure (video, voice, and data). Installs, operates, and maintains Local Area Networks (LANS) and Wide Area Networks (WANS). Maintains network security of routers and transmission systems and troubleshoots physical layer network problems. As the primary staff officer for all automation network support, network policy and ABCS support, the G6/S6 is responsible for:

- Monitor/manage the WAN/LAN performance/connectivity
- Managing/monitoring software releases of ABCS/STAMIS operating system within the battalion, brigade, and division
- Overseeing the planning and installation of the LAN configuration procedures
- Planning, engineering and managing the tactical internet/Tactical LAN
- Implementing and enforcing LAN security policies
- Network Configuration
- Automation Training on network devices such as: routers, hubs, switches, etc…) NOT RESPONSIBLE FOR APPLICATION SOFTWARE TRAINING!

- Implementing and training response teams to provide on site support
- Determine preventive measures that must be employed to secure the information that networks and information systems pass and store. (See AR 380-19, AR 25- Information Assurance (IA) dtd. December 1999, AR 380-5, and Army Tactical Network and Information Systems Information Assurance Concept of Operation, dtd. 08 September 00, ver. 0.8)

AUTOMATION OFFICER (AO)

AO is a functional staff organization within the Division G6 section. This staff element provides the division with support for C2 systems (ABCS). AO plans, organizes, and coordinates all tactical automation to support the division commanders C2 systems (ABCS). AO establishes automation systems administration procedures for all automation software and hardware employed by the division, coordinates the configuration of the communications network that supports the division, and establishes automation system security for all automation software and hardware employed by the division.

SUPPORT COMMAND

Support Commands at all levels have unique staff sections not found in other commands. These staff sections are listed below along with their duties and responsibilities for automation and combat service support.

S2/S3

Within the support commands of the corps and division, the S2 and S3 sections are typically consolidated. The S2/S3 is the principal staff advisor to the support command commander on military intelligence, counterintelligence, organization, training, communications, and Nuclear, Biological and Chemical (NBC) matters. The S2/S3 will:

- Determine Division Support Command (DISCOM) unit readiness and mission capability.
- Plan/monitor operator sustainment training
- Provide operational and support guidance to subordinate units
- Coordinate with the S6 for communications connectivity
- Supervise the command security program and evaluate security vulnerabilities
- Assist the S6 in implementing and enforcing LAN security policies

SUPPORT OPERATIONS

The Support Operations Officer is responsible for providing division units with centralized, integrated and automated command, control, and planning for all logistical distribution management operations within the division. He ensures that supply, maintenance, transportation, and field services resources are used effectively. He provides management support and direction to DISCOM assets responsible for providing logistics. Management includes planning, coordinating, and controlling the allocation and use of available resources to fulfill the DISCOM commander's logistics requirements. The support operations officer also:

- Develops administrative plans and coordinates logistics plans.
- Recommends priorities for allocating logistical/support resources.
- Maintains coordination with reinforcing maintenance units, to include the Electronic Sustainment Support Center (ESSC).
- Articulates support priorities to the reinforcing maintenance units and the ESSC to facilitate the repair and return of the most critical equipment.
- Advises the Commander on problems affecting supply, maintenance, transportation, and field service operations.
- Recommends to the S2/S3 the future allocation and location of logistics elements.
- Plans, coordinates, and evaluates supply and maintenance operations.
- Coordinates, monitors, and informs supported units of the location of supply points.
- Determines requirements for the development and technical supervision of division authorized stockage lists. Requirements are determined in accordance with AR 710-2, associated pamphlets, and automated systems users manuals.
- At the DISCOM level, manages the division master property records. It establishes and maintains a centralized division property book for all divisional units.
- Manages maintenance workload of corps reinforcing units and Maintenance Support Teams (MSTs) in support of the division, when located in the division area.
- Advises the commander on the status of maintenance and repair parts.

Combat Service Support Automation Management Office (CSSAMO).

THEATER SUPPORT COMMAND (TSC), CORPS SUPPORT COMMAND (COSCOM).

CSSAMOs located at the Theater Support Commands and COSCOMs serve in a supervisory role to all subordinate CSSAMOs. They establish CSS automation policy and provide guidance for all the CSSAMOs in the command. They coordinate actions and serve as the systems integrator for the command. They are the focal point for all new system fieldings, software changes, engineer change proposals and any other CSS automation actions requiring coordination between agencies, within and outside the commands.

AREA SUPPORT GROUP (ASG), CORPS SUPPORT GROUP (CSG), DISCOM, ARMORED CAVALRY REGIMENT (ACR)/SEPARATE BRIGADES.

The CSSAMO provides customer support in operating and sustaining the Army's CSS Standard Army Management Information Systems (STAMIS). This includes support for all application software, limited hardware repair, monitoring user training programs, and new equipment fielding of STAMIS. The CSSAMO is responsible for the following tasks:

- Provides STAMIS application and operating system support
- Provides software configuration management and control
- Provides database management support
- Maintains tape libraries
- Develops temporary workarounds
- Tests users suggestions
- Conducts customer assistance visits
- Assists units during deployments
- Task organizes resources to support deployments
- Troubleshoots HW/SW problems
- When required, maintains hand receipts and STAMIS Computer Exchange (SCX) Line Replaceable Units (LRUs)
- Coordinates repair of SCX LRUs
- Coordinates closely with the G6/S6 on STAMIS software implementation and changes
- Receives, issues and controls all STAMIS software releases
- Operates the STAMIS help desk

SIGNAL BATTALION

The signal battalion supports the division (brigade combat teams, separate battalions, division support command (DISCOM) (CSSAMO), and division headquarters (division rear, division main, tactical command posts, and support area)) by maintaining its communications systems in order to support division level combat functions, which include C2 (ABCS), STAMIS (Global Combat Support System-Army (GCSS-Army)), and CSS.

The signal battalion controls the data transport systems used to transmit ABCS and STAMIS data internal/external to the division. The degree of success in providing the division commander quality C2 (ABCS) and accurately forecasted logistical support (STAMIS/CSS) depends on the availability and success of transmission to and from these systems. The signal battalion must provide ABCS, STAMIS, and CSS the ability to receive, process, and transmit information.. The signal battalion must provide a communications network that's configured properly and interfaced at the appropriate level. How well the signal battalion accomplishes these tasks has a direct effect on accomplishing the commander's intent.

AUTOMATION SUPPORT PERSONNEL

The relationship between the various officer, warrant officer, and enlisted Military Occupational Specialties (MOSs) is crucial to the total support of the division's communications and automation systems.

The MOSs and additional duties listed below have uniquely different responsibilities; they each play an important part in maintaining automation on the battlefield.

MOS 31U

The 31U, Signal Support Systems Specialist supervises, installs, employs, maintains, and troubleshoots Signal support equipment systems and terminal devices. He is trained to operate and support a wide variety of electronic, communications, communications security (COMSEC), and automated systems. The 31U is located within the various battalion and brigade S6 sections and also within the Signal battalion. As a part of the S6 section, the 31U is located where he can best provide support to the unit's communications and automation systems. The sections are centralized at the battalion/brigade headquarters facilitating signal support planning and training. However, the section is flexible enough to allow task organization of the 31U to support individual unit requirements. This enables the 31U to assist units with communications and automated systems training and preventive maintenance checks and services (PMCS).

MOS 74B

The 74B, Information Systems Operator-Analyst supervises installs, operates, and performs unit level maintenance on network servers, multifunction and/or multi-user information processing systems, peripheral equipment, and associated devices in mobile and fixed facilities. The 74B can troubleshoot the entire spectrum of the network, hardware and software. Additionally, the 75B performs analyst, system administrator, and LAN management functions. Combined with the 31U, the 74B gives the S6 section the capability of troubleshooting and repairing most network and computer problems. The 74B is located within the battalion/brigade S6 sections, G6 section, the Signal battalion, and the division CSSAMO.

MOS 35J

The 35J, Computer/Automation System Repairer performs or supervises the direct support (DS) and general support (GS) levels of maintenance on microcomputers and electromechanical telecommunications terminal equipment, facsimile machines, field artillery (FA) digital devices, and other associated equipment and devices. The 35J is located within the Base Support Company (BSC), the Area Maintenance Company (AMC), the Ground Maintenance Company (GMC), and the non-divisional maintenance company.

MOS 250N

The 250N, Network Management Technician manages plans, designs, engineers, installs, operates, maintains, and evaluates automation communications at all command levels within the Department of the Army and Department of Defense. The 250N is responsible for the operation of message, circuit, and data-switching networks at all echelons: division, corps, joint task force, theater, and sustaining base. He coordinates network interface protocols and procedures with those of other services and combined forces, and coordinates network troubleshooting and restoration of communications paths to maintain robust networks. The network management technician implements procedures for detecting and reporting COMSEC insecurities and recommends compromise recovery actions. He develops policy and provides guidance for management of division and above and joint task force networks. He provides technical guidance and direction to subordinate operating elements. The 250N develops and supervises the training of network management personnel. The 250N is located at brigade and above level in selected units throughout the division.

MOS 251A

The 251A, Information Systems Technician manages personnel and equipment assets associated with AISs and Internet protocol (IP) networks to include the internetworking of systems. The 251A is trained to perform configuration management of the AIS network hardware installation and integration of information systems into tactical networks. To ensure system security, the 251A implements and supervises security training and awareness programs and conducts AIS security inspections. The 251 is responsible for systems administration of tactical AISs in the division; manages training of personnel in the installation, operation, administration, and maintenance of tactical AISs, internet works, and video teleconferencing systems. He provides technical guidance and direction and helps develop maintenance programs to subordinate operating elements. The 251A is located at brigade and above level in selected units throughout the division.

FUNCTIONAL AREA (FA) 53

FA 53, Systems Automation Manager manages computer systems and provides automation expertise at all Army organizational levels to include joint, combined, and selected agencies. FA 53 officers assist commanders with a variety of automation services. FA 53 officers translate mission needs into defined computer systems requirements; advise on all automation policy and technical matters; perform economic analyses; plan, program, and budget for automation resources and logistic support; establish procedures for effective and efficient use of computer system resources; and plan and manage LANs. A FA 53 officer heads the CSSAMO in the division. The FA 53 officer is located in brigade and above staff elements.

MOS 25A

The 25A signal officers understand the Army's information system networks and the connectivity between different information systems. They are technically proficient with branch and mission-unique equipment, tools, and systems. The 25A officer is located throughout the division down to the platoon level.

INFORMATION MANAGEMENT OFICER (IMO)

The IMO is responsible for the support automation within an Organization. This function is an additional/special duty that is assigned to an individual. This position does not require any formalized school training, specific MOS or rank.

MISSION APPLICATION ADMINISTRATOR (MAA)

The MAA provides the using units with the expertise to assist the Mission Application User (MAU) to operate, maintain, and troubleshoot failed hardware and software systems. He also trains the MAU on the units/battlefield FA specific AISs. The MAA—

- Assists the MAU in troubleshooting.
- Monitors the Preventative Maintenance Checks and Services (PMCS) program.
- Monitors software applications and configuration management.
- Maintains master copies of his battlefield functional area (BFA) specific software

- Creates backups of the BFA AIS data.
- Assists the MAU in recovery of data.
- Coordinates automation support with the S6 section.

Note: This position is an additional duty and is not a standard TOE duty position.

MISSION APPLICATION USER (MAU)

The MAU provides the BFA with the capability to operate and maintain the specific AIS. The MAU is the best trained to provide systems specific application automation support. The MAU—

- Installs the AIS.
- Operates the AIS.
- Performs backups and recovery of files.
- Performs PMCS.
- Performs operator level security.
- Performs unit level maintenance on ABCS, STAMIS, and support automation.
- Prepares continuity plans for degraded operations.

Hardware/Software and Support Automation Procedures

Units cannot afford to have systems down for any significant period of time. Continuous improvements in technology and extensive fielding of new equipment have made logistical automation support increasingly difficult. Support is also further complicated by the increased involvement of contractors on the battlefield. Many computers today, particularly C2 devices, are supported through unique, stovepipe systems. These stovepipes often involve a mix of military, civilian, and contractor personnel for both maintenance and supply support. This chapter discusses ABCS, STAMIS, and support automation procedures.

ARMY BATTLE COMMAND SYSTEM (ABCS) SUPPORT

ABCS equipment is currently supported through a variety of maintenance concepts and warranties. The majority of ABCS systems is purchased through the common hardware/software (CHS) program. The CHS-2 platforms are the most modern, upgraded configurations and are scheduled to replace the CHS-1 systems.

The CHS-2 hardware is supported through a two-level maintenance concept. The current Army maintenance program is a flexible, four-level system. The levels are operator/unit, direct support (DS), general support (GS), and depot. Currently selected units supported under Force XXI designs have merged the existing 20/30 maintenance levels. Units of Army XXI design will migrate into a two-level maintenance structure where maintenance functions are consolidated into either field or sustainment maintenance levels.

Field maintenance support includes operator/unit, direct support (DS), and some component repair capability designed to repair components and end items for customer units versus the supply system. The multicapable maintainer is the cornerstone of field maintenance support. This individual is trained to perform both unit and DS tasks to improve system readiness and reduce repair cycle time. Field level maintenance is performed by the unit and is characterized by Line Replaceable Unit (LRU) removal and replacement. LRUs are covered by a life of the contract warranty and repaired by the contractor. For the ABCS central processing units (CPUs), monitors, printers, keyboards, interconnecting cables, external drives, and mouse/pointing devices are considered LRUs.

Sustainment maintenance support includes depots, Directorate of Logistics (DOL) assets, special repair activities (SRAs), and forward repair activities (FRAs). There are also a limited number of specialized GS units that provide missile and signal unique support.

The G6/S6 sections also assists units in maintaining ABCS. Figure 3-1 shows the general flow of maintenance support for ABCS.

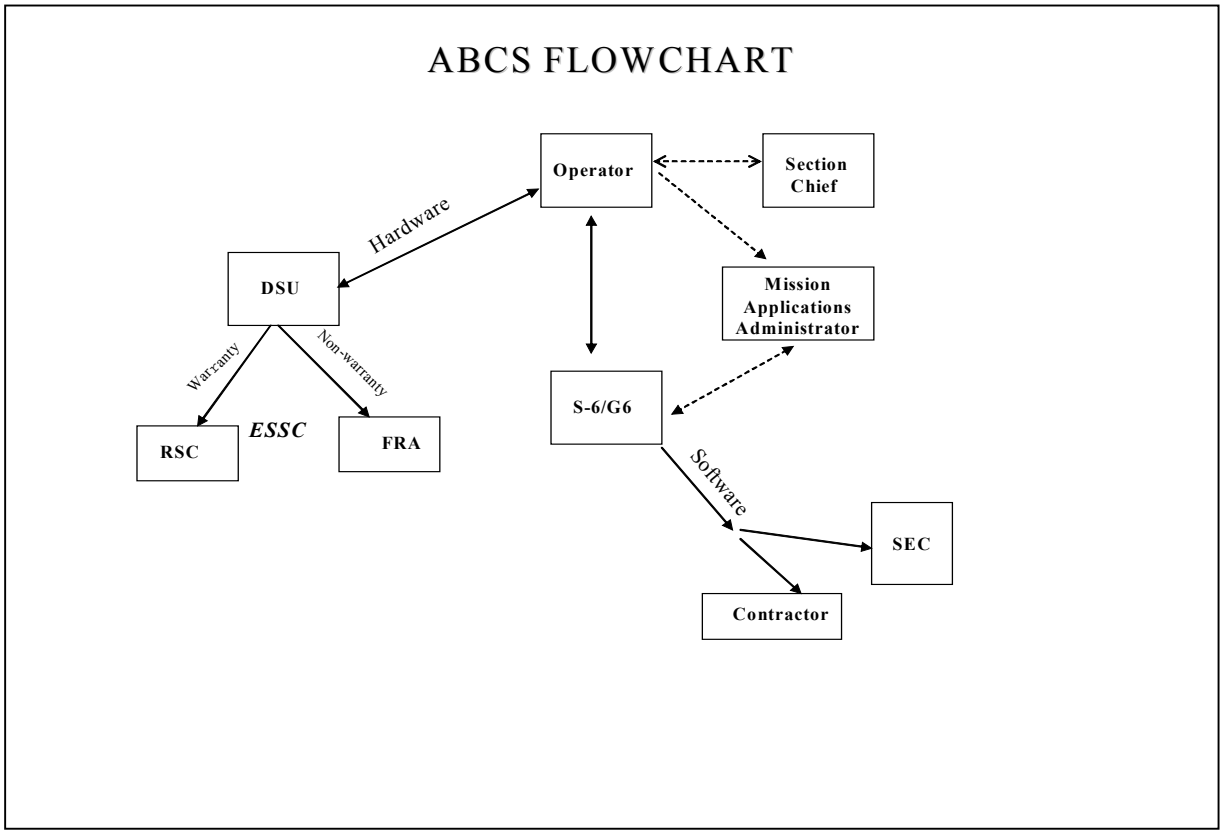

Figure 3-1 ABCS Flowchart

ABCS- BRIGADE SUPPORT AREA (BSA) PROCEDURES

The support procedures within the BSA (Figure 3-2), DS supply, and maintenance are consolidated within the BSC. The FSC receives unserviceable LRUs from unit personnel and processes their requests for replacement LRUs and consolidates distribution to the BSC. The FSC also receives replacement LRUs from the BSC and issues them to the MAU.

The BSC screens all LRUs to determine if the systems are covered by warranty. Warranted LRUs will be managed as repairable exchange using “off-line” manual procedures. ***Note:*** This is necessary to provide a no cost issue to the unit. Current supply/financial systems interface will not allow for free issue. GCSS-A will remedy this issue when fielded. For warranted and non-warranted LRU repair see Table 3-1.

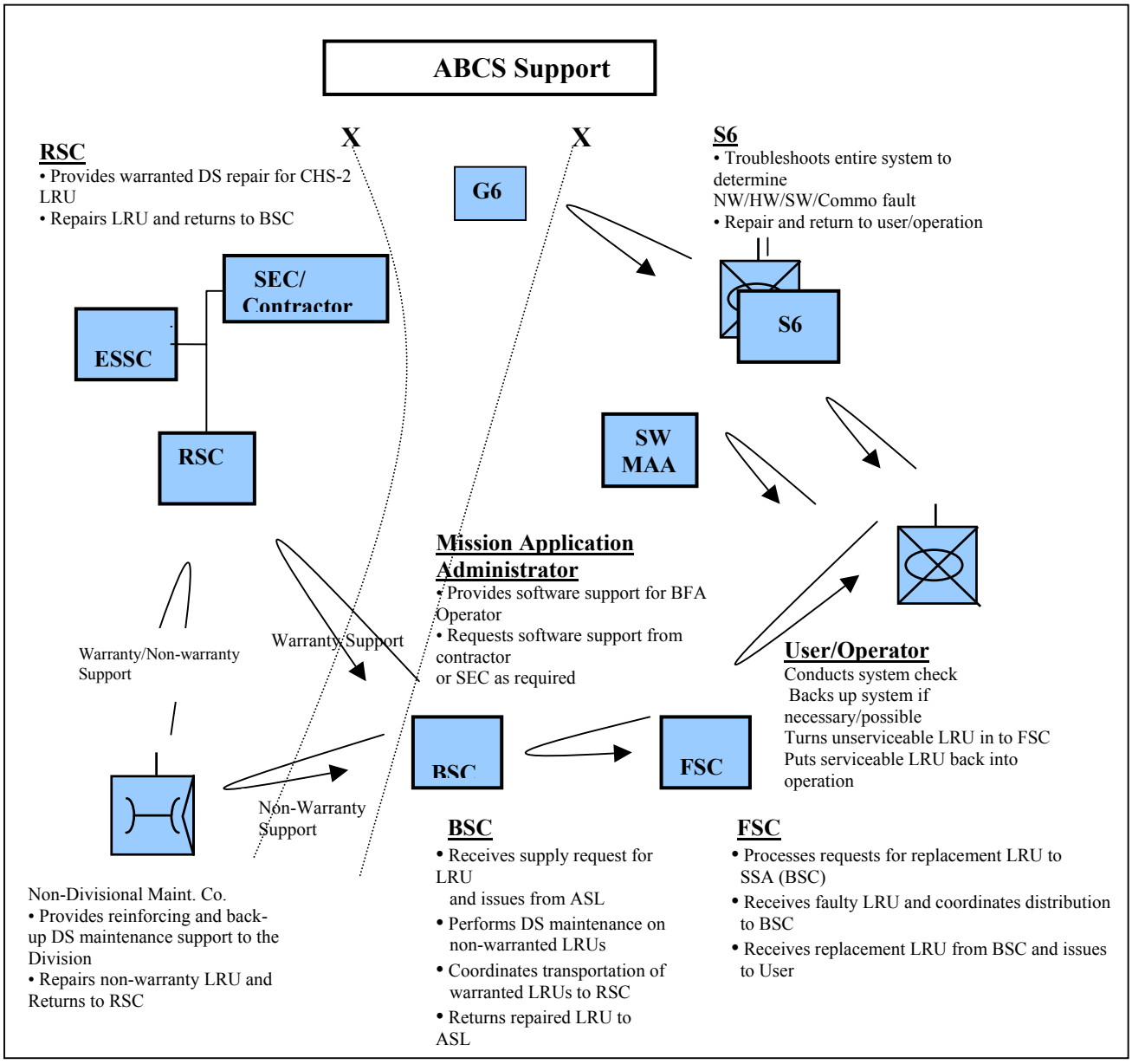

Figure 3-2. ABCS-BSA Support Procedures

ABCS-Division Support Area (DSA) procedures

The support procedures within the DSA differ slightly from the BSA (Figure 3-2). In the DSA (Figure 3-3), DS supply and maintenance are not consolidated within a single company such as the BSC. Within the DSB, the AMC provides DS maintenance to other DSB units, the Signal battalion, the air defense artillery (ADA) battalion, the military intelligence (MI) battalion, the Multiple-Launch Rocket System (MLRS) battalion, and other division rear units. The DSB quartermaster (QM) company operates the SSA. Within the division aviation support battalion (DASB), the GMC provides DS maintenance to other DASB units, the division aviation

brigade, and the division cavalry squadron. The DASB headquarters and supply company operate the SSA.

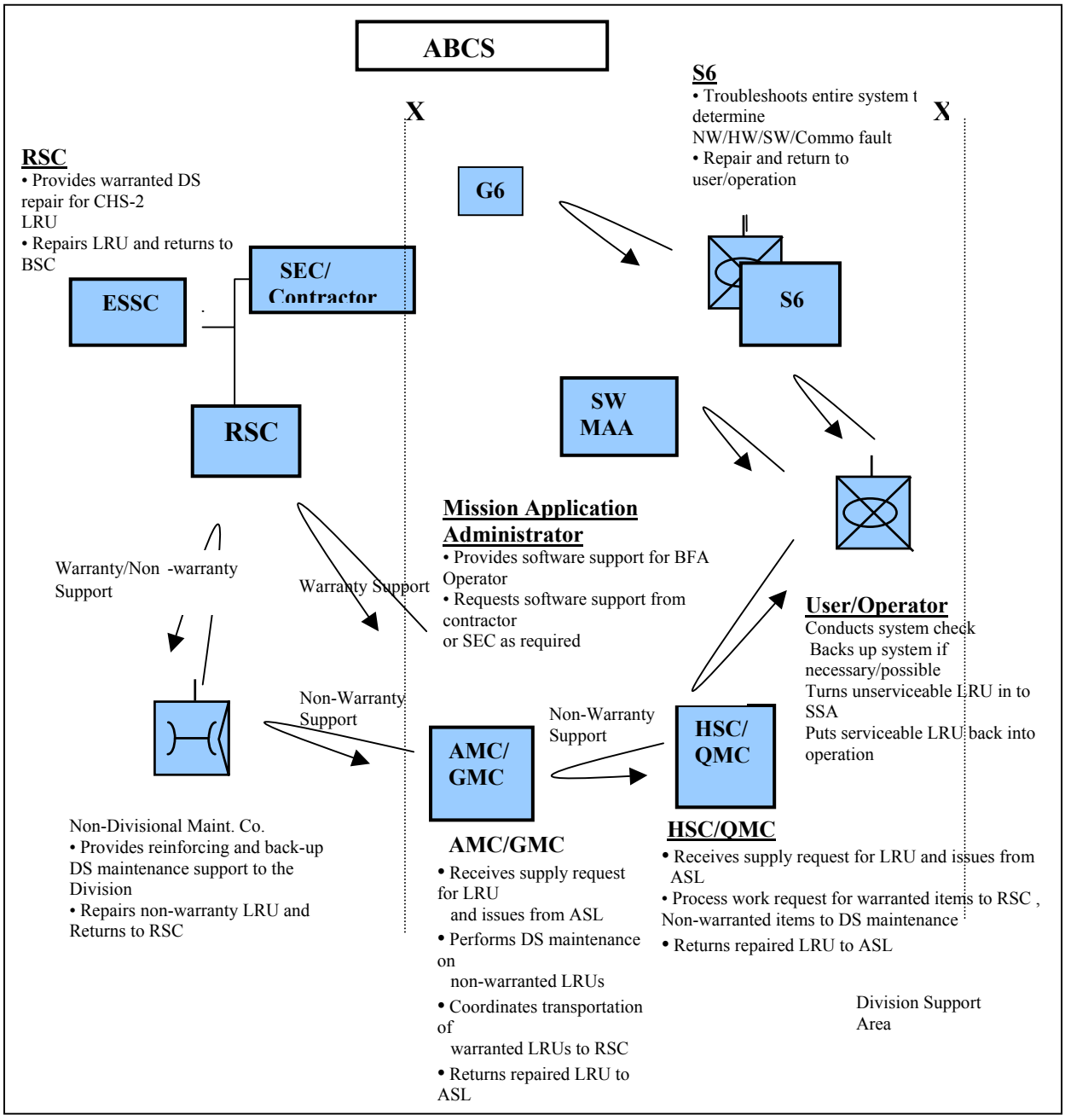

Figure 3-3. DSA Support Procedures

ABCS-ECHELONS ABOVE DIVISION (EAD) PROCEDURES

ABCS support at EAD follows similar procedures as the support within the division area. Figure 3-4 shows the notional support for corps ADA units. The battalion S6 section provides unit level troubleshooting assistance to ABCS MAUs.

The non-divisional maintenance company provides DS supply and maintenance support for the battalion. The non-divisional maintenance company provides support to corps units on an area basis.

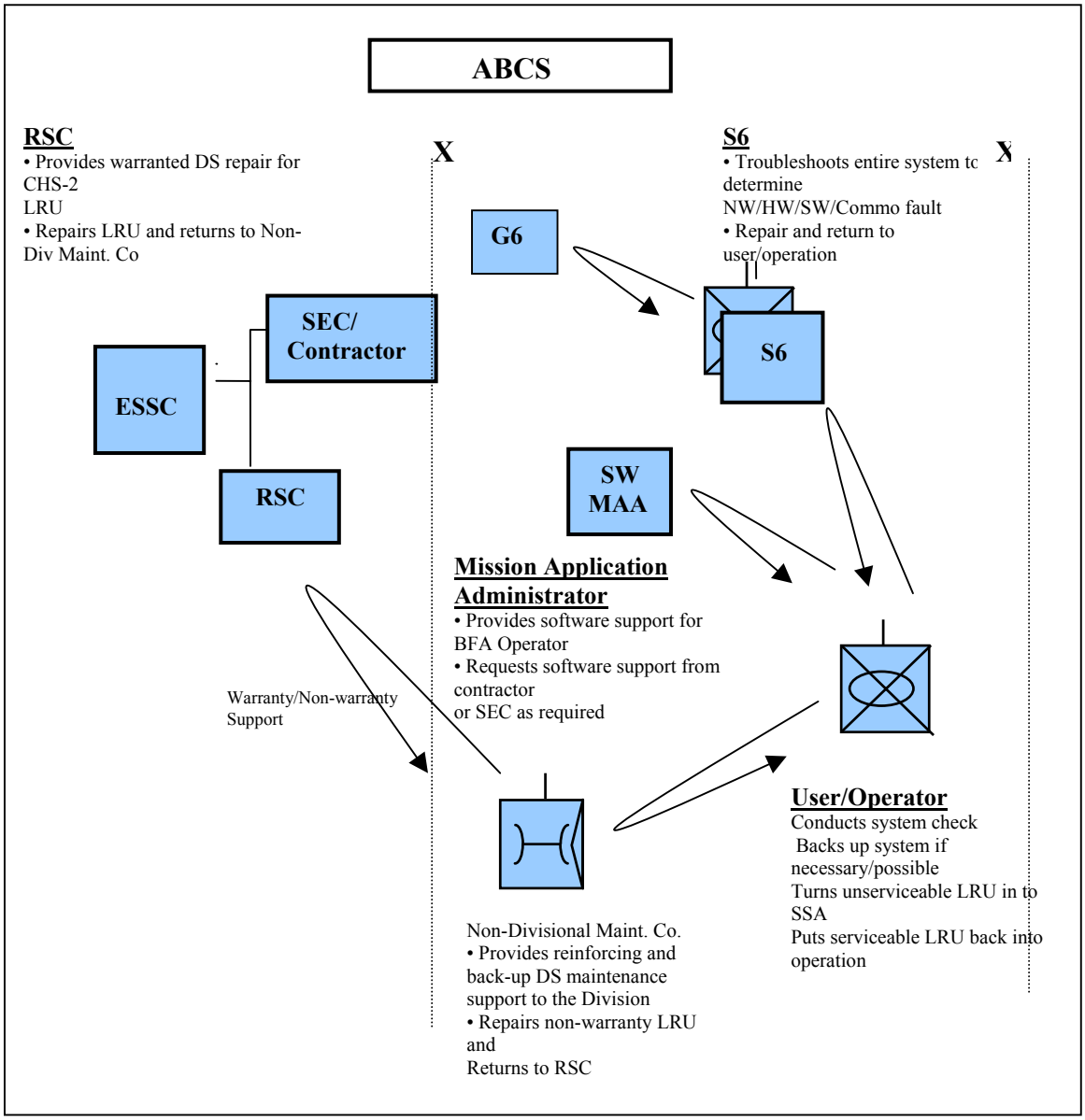

Figure 3-4. ABCS Support for EAD

Table 3-1 lists the troubleshooting procedures for ABCS (BSA/DSA/EAD).

Table 3-1. Troubleshooting Procedures for ABCS (BSA/DSA/EAD)

Step	Procedure
1	**The MAU discovers a fault**
	The MAU determines the system to be nonoperational and notifies the MAA/section chief of a system failure. Using diagnostic software and built-in-test equipment, the MAU and MAA will try to determine whether the failure is software, hardware, or network related. For software related problems, the MAU will reload the software (provided software and skill sets are available) and return the system into operation.
2	**MAA troubleshoots**
	The MAU/MAA cannot correct the problem or determines the problem to be a network/communications-related failure; he will contact the S6.
3	**The S6 is notified—**
	1. The S6 will troubleshoot the system and identify the failure as software (step 4), hardware (step 5), or network (step 6) problem. Upon completing the troubleshooting procedures, the S6 assists the MAU/MAA in– • Restoring the system by reinstalling system/application software. • Identifying/verifying the malfunctioning LRU. • Identifying problems in the LAN connectivity. 2. The S6 cannot restore the system; the unit turns in the LRU to the FSC. 3. The S6 requests assistance from the G6 for LAN connectivity problems when required.
4	**Software**
	If the problem is software and reinstalling the system application does not correct the fault, the S6 will direct the unit to contact their next level of software support (ex. Bde/Div MAA) and/or the S6 will consult the G6 for additional assistance in fault isolation and repair.
5	**Hardware**
	The S6 identifies the problem to be a malfunctioning LRU and cannot repair it. The S6 will direct the unit to turn the unserviceable LRU into the ~~FSC~~ Maintenance Company, or the S6 will consult the G6 for additional assistance in fault isolation and repair. The MAU will request replacement LRUs and turn in the failed LRU through the supporting– • FSC if at the BSA. • SSA if at the DSA/EAC.
6	**Network/LAN connectivity**
	If the fault is determined to be in the LAN and the proper tools and/or skill set(s) are not available for the S6 to repair the fault, the G6 will assist the S6 in repairing LAN connectivity problems.

Table 3-1. Troubleshooting Procedures for ABCS (DSA/BSA/EAD) (continued)

Step	Procedure
7	**Warranted LRUs**
	For warranted LRUs, the SSA processes a work request to the appropriate RSC. Based on the maturity of the theater of operations, the BSC may process warranted items through the non-divisional maintenance company. Elements of the RSC typically deploy as part of CECOM's ESSC. The RSC will repair all warranted LRUs and return them to the SSA. The SSA returns the item to the user or supply.
8	**Nonwarranted LRUs**
	Non-warranted systems will require coordination between the FSB support operations section, the BSC, and the supporting non-divisional maintenance company. This coordination is required to determine the appropriate repair facility based on the unit's maintenance backlog, personnel, and test equipment available. The SSA will work order the LRU to the appropriate unit for repair. At the BSC/AMC/GMC, maintenance personnel will conduct a technical inspection to verify failure. When a failure exists, the DS maintainer will perform all authorized repair actions to restore the LRU to a serviceable condition. These procedures may involve the use of operating system tools, diagnostic software, and school-taught repair skills. Nonwarranted LRUs will be managed as repairable exchange. The repaired LRU will be returned to the SSA or returned to the customer for completed work requests. The BSC/AMC and GMC may also evacuate excess workload to the non-divisional maintenance company.
9	**Non-divisional maintenance company**
	The non-divisional maintenance company provides DS maintenance support to units on an area basis. DS maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. The non-divisional maintenance company will return all serviceable LRUs to the customer. Additionally, the unit provides reinforcing and backup DS maintenance to the– • BSC if at the BSA. • AMC and GMC if at the DSA. • SSA if at EAD. **Note: Figure 3-3 shows the general flow of ABCS support for the DSA.**
10	**ESSC**
	The ESSC provides warranty/nonwarranty support. Contractor maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. They also provide support in shipping distribution back to the manufacturer when further repairs are needed. The ESSC returns all serviceable LRUs to the SSA . **Note: Figure 3-2 shows the general flow of ABCS support for the BSA. Figure 3-4 shows the general flow of ABCS support for the EAD.**

STANDARD ARMY MANAGEMENT INFORMATION SYSTEM (STAMIS) SUPPORT

STAMIS equipment currently operates on standard, Common off the Shelf (COTS), and non-developmental items (NDI) hardware and software. STAMIS hardware is fielded with a manufacturer warranty for DS level repairs. The Depot Forward Repair Activity (FRA) maintains warranty information for all supported STAMIS equipment. The FRA either repairs or facilitates the distribution and repair of all warranted STAMIS hardware. The FRA also performs all non-warranty repair of STAMIS hardware.

STAMIS basically follows a two-level maintenance concept: The first level of maintenance is performed by the CSSAMO and consists of basic diagnostics and exchange of Line Replaceable Units (LRU). The CSSAMO will have the ability to perform basic diagnostics in an attempt to determine which LRU has malfunctioned. Once the LRU has been isolated, the CSSAMO will exchange the malfunctioning LRU.

The second level of maintenance consists of the CSSAMO evacuating the faulty LRU to either a Forward Repair Activity (FRA) or the manufacturer. If the LRU is still under warranty, it will be forwarded the manufacturer for repair or exchange. If the LRU is out of warranty, it will be forwarded to the designated FRA for repair. If the LRU cannot be repaired by the FRA, the LRU will be returned to the CSSAMO for turn-in and purchase of a replacement.

The general maintenance flow is shown in Figure 3-5. The S6 provides unit level maintenance for network problems. The CSSAMO provides detailed software application support (Figure 3-6) and manages the STAMIS Computer Exchange (SCX) account. The FRA for hardware and the STAMIS Customer Assistance Office (CAO) provide DS maintenance for software applications. Table 3-2 list STAMIS support procedures.

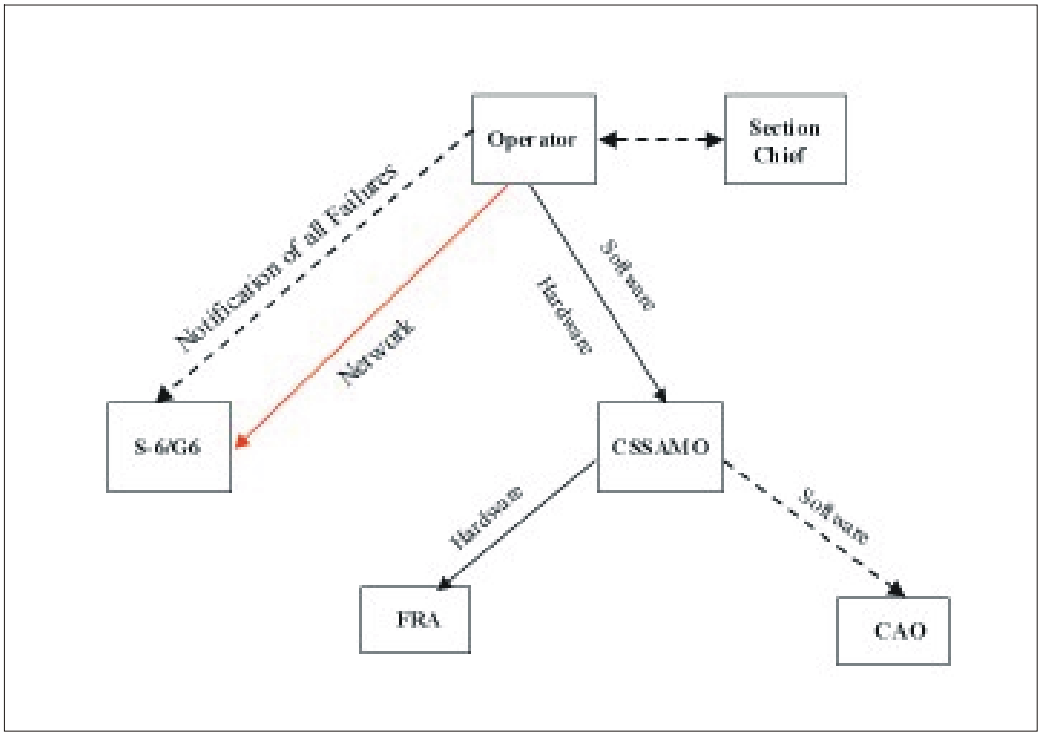

Figure 3-5. STAMIS Flowchart

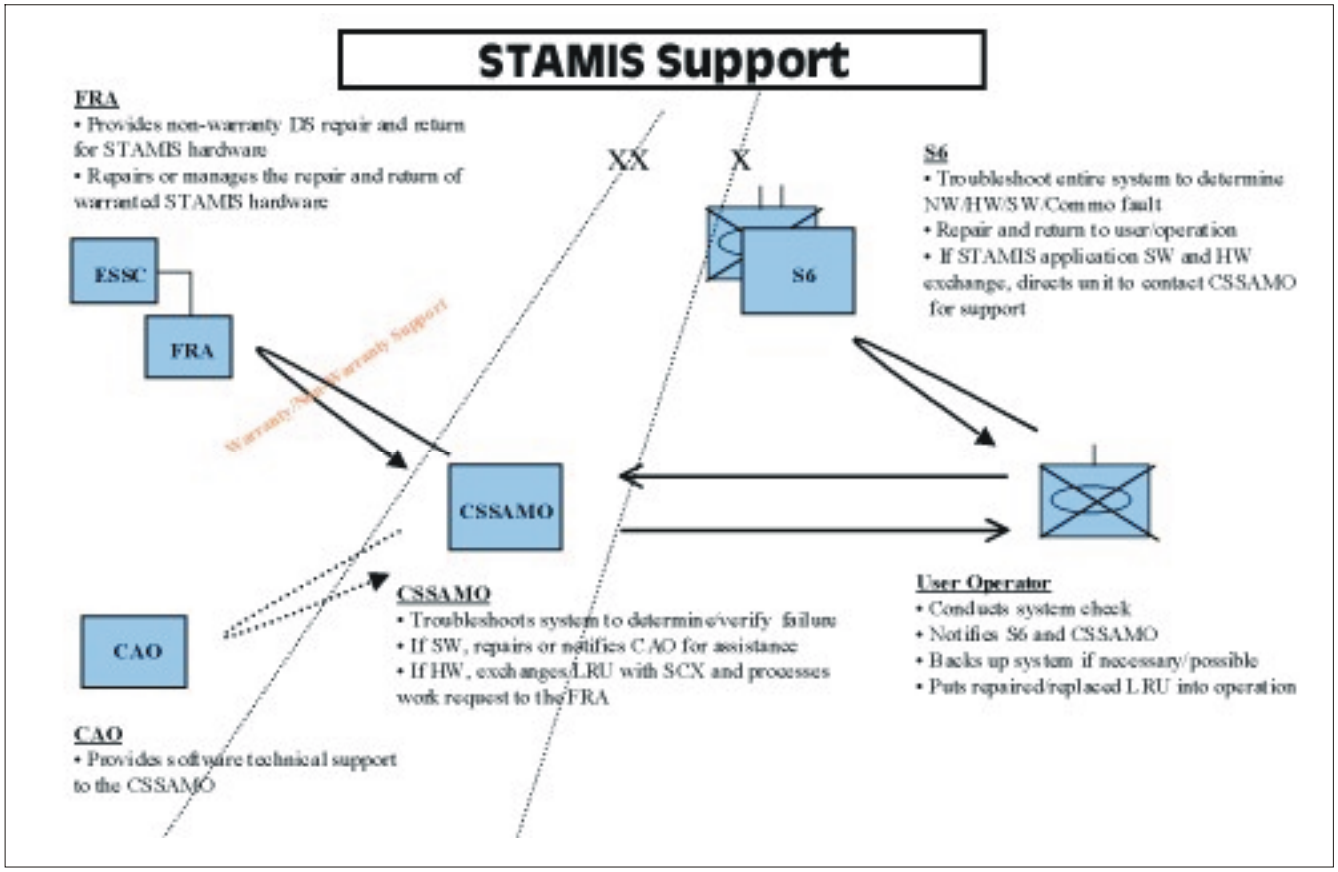

Figure 3-6. STAMIS Support Flowchart

Table 3-2. STAMIS Support Procedures

Step	Procedure
1	**The MAU discovers a fault**
	The MAU determines the system to be non-operational and notifies the MAA/section chief of a system failure. Using diagnostic software and built-in-test equipment, the MAU and MAA will try to determine whether the failure is software, hardware, or network related. For software related problems, the MAU will reload the software (if available) and return the system into operation. MC4 is a software application that provides for “restore disk” capability by the MAA or designated Enterprise Manager.
2	**MAA troubleshoots**
	The MAU/MAA cannot correct the problem or determines the problem to be a network/communications-related failure; he will contact the S6.

Table 3-2. STAMIS Support Procedures (continued)

Step	Procedure
3	**The S6 is notified—**
	1. The S6 will troubleshoot the system and identify the failure as software (step 4), hardware (step 5), or network (step 6) problem. Upon completing the troubleshooting procedures, the S6 assists the MAU in– • Restoring the system by reinstalling system/application software. • Identifying/verifying the malfunctioning LRU. • Identifying problems in the LAN connectivity. 2. The S6 requests assistance from the G6 for LAN connectivity problems when required. 3. If the S6 cannot resolve the problem, the CSSAMO will be contacted. The CSSAMO will troubleshoot the system to determine if the failure is software (step 4), hardware (step 5), or network (step 6) problem.
4	**Software**
	1. The CSSAMO will troubleshoot the software application and operating system and attempt to restore the system to an operational condition. For repairs beyond their capability, the CSSAMO will notify the STAMIS CAO. The CAO will provide the technical support necessary to restore the system to an operational condition.
5	**Hardware**
	For hardware faults, the CSSAMO will first verify failure and identify the faulty LRU. The CSSAMO will exchange LRUs with the supported unit from SCX stocks. The CSSAMO will process the work order and request disposition instructions from the FRA. MC4 equipment is not a repairable platform using Line Replaceable Units (LRU) and is considered a complete system or Shop Replaceable Unit (SRU). Computer exchange is the only authorized action to be performed for replacement purposes.
6	**Network/LAN connectivity**
	If the fault is determined to be in the LAN and the proper tools and/or skill set(s) are not available for the S6 to repair the fault, the G6 will assist the S6 in repairing LAN connectivity problems.
7	**Warranted LRUs**
	For warranted LRUs, the FRA may direct the CSSAMO to return the LRU to the original equipment manufacturer.
8	**Nonwarranted LRUs**
	For nonwarranted LRUs, the CSSAMO will process a work order with the FRA. Once the items are repaired, the CSSAMO will return the LRUs to SCX stockage.

Table 3-2. STAMIS Support Procedures (continued)

Step	Procedure
9	**Electronic Sustainment Support Center (ESSC)**
	The ESSC provides warranty/non-warranty support. Contractor maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. They also provide support in shipping distribution back to the manufacturer when further repairs are needed. The ESSC returns all serviceable LRUs to the CSSAMO.

SUPPORT AUTOMATION

Support automation describes all computers and ADPE used to support a unit's operation (less ABCS and STAMIS). Appendix A provides a description of support automation.

With some exceptions, the TDA or CTA authorizes support automation. This equipment is normally covered by a manufacturer's warranty. While warranties differ in terms of coverage and length, most do not apply when units deploy.

Units have two options for support of support automation: organic support and a mixture of organic and contract support.

ORGANIC SUPPORT

First option, organic support relies on the unit information management officer (IMO) and the S6 for unit level maintenance. Unit level maintenance involves the removal and replacement of LRUs. LRUs consist of CPUs, monitors, printers, external drives, keyboards, pointing devices, and cables. DS maintenance is provided by selected DS maintenance activities and involves the repair of LRUs. Repair is accomplished by the removal and replacement of shop replaceable units (SRUs). DS repair can only be accomplished through the provisioning of spare SRUs and selected components. Units may also utilize local purchase procedures to acquire the necessary SRUs

ORGANIC AND CONTRACT SUPPORT

Second option entails a mix of organic and contract support. Unit IMOs and S6 sections provide unit level hardware and software support. Software support consists of operating system diagnostics and other utility applications. For hardware, unit level repair consists of removal and replacement of LRUs. The FRA provides DS maintenance through a reimbursable contract. This procedure is shown in Figures 3-7 and 3-8. Table 3-3 list organic support procedures.

Note: The provisioning of spare LRUs as far forward (BSC/FSC/combat repair teams (CRTs)) as possible on the battlefield significantly reduces travel and repair time, which ultimately increases readiness.

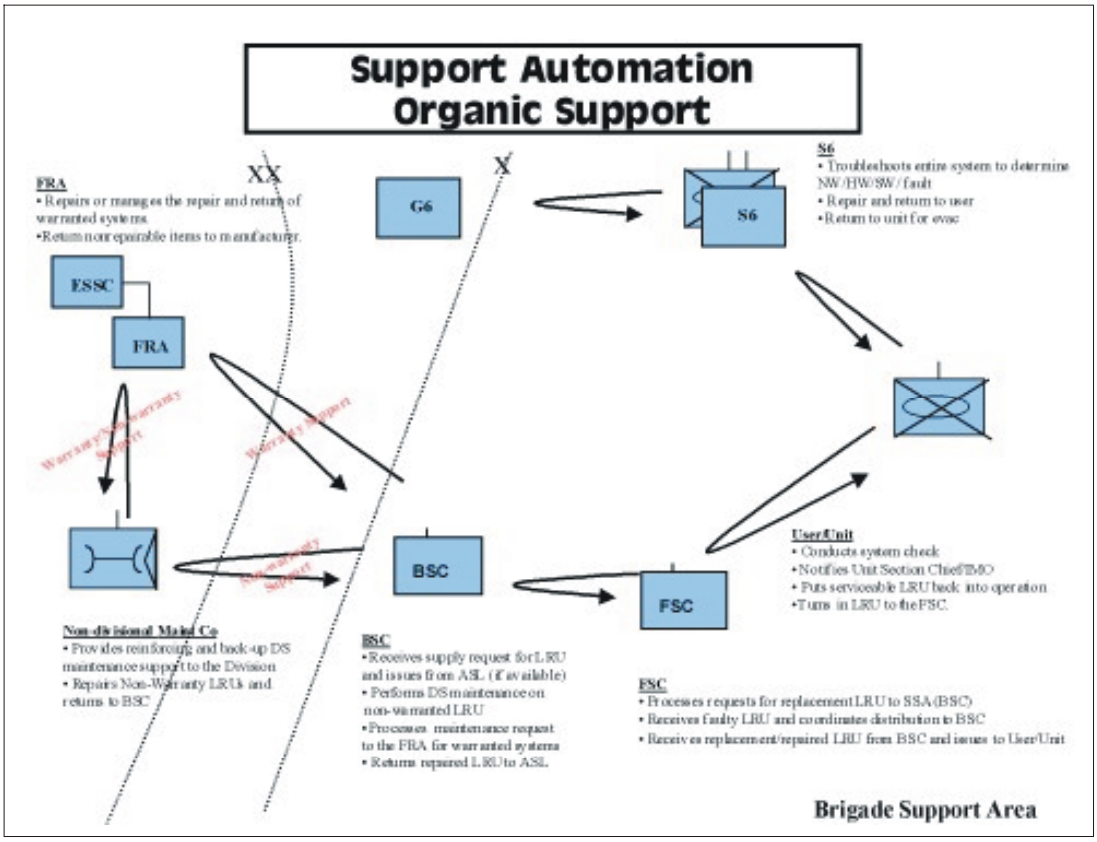

Figure 3-7. Organic Flowchart

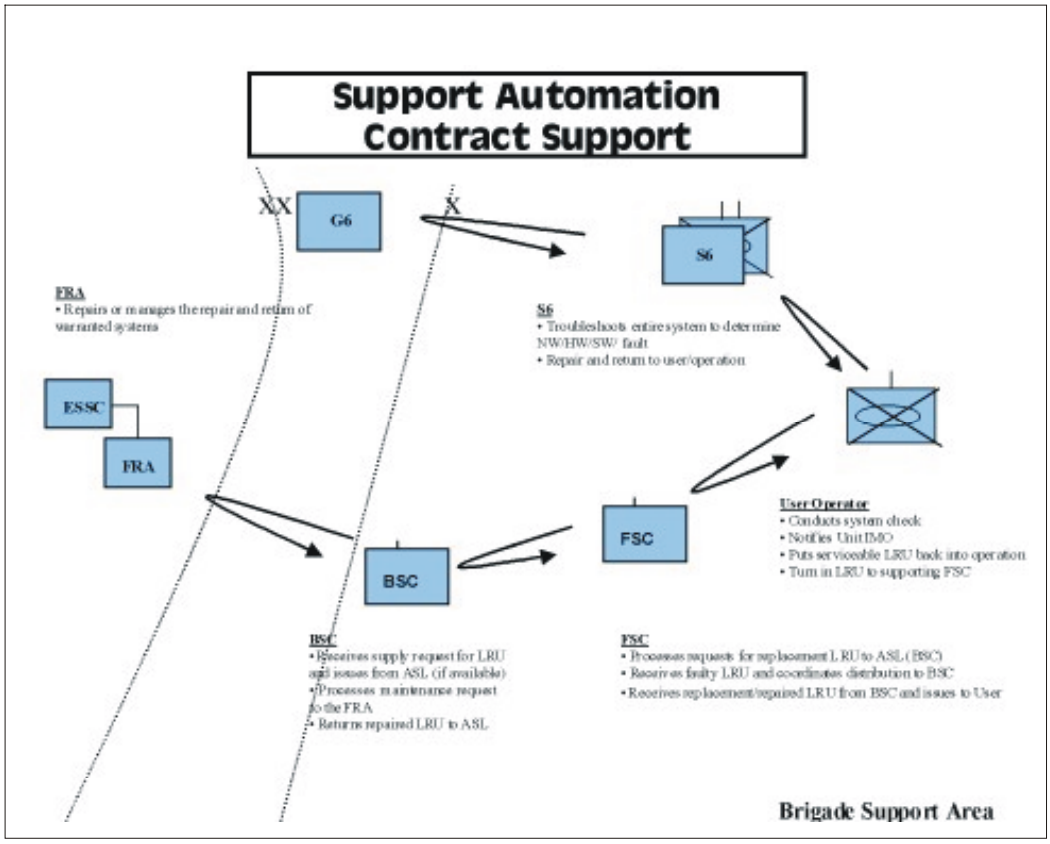

Figure 3-8. Contract Flowchart

Table 3-3. Support Automation–Organic Support Procedures

Step	Procedure
1	**The MAU discovers a fault**
	The MAU determines the system to be non-operational and notifies the IMO of a system failure. The MAU and IMO will try to determine whether the failure is software, hardware, or network related. The unit IMO will provide intensive troubleshooting and attempt to return the system to operation.
2	**MAU/IMO troubleshoots**
	If the MAA/IMO cannot correct the problem, they will contact the S6 section for assistance.

Table 3-3. Support Automation-Organic Support Procedures (continued)

Step	Procedure
3	**The S6 is notified—**
	1. The S6 will troubleshoot the system and identify the failure as software (step 4), hardware (step 5), or network (step 6) problem. Upon completing the troubleshooting procedures, the S6 assists the MAU in– • Restoring the system by reinstalling system/application software. • Identifying/verifying the malfunctioning LRU. • Identifying problems in the LAN connectivity. 2. The S6 cannot restore the system; the unit turns in the LRU to the FSC. 3. The S6 requests assistance from the G6 for LAN connectivity problems when required. The S6 will verify the status of the automation system and attempt to identify the failure as a software (step 4), hardware (step 5), or network (step 6) problem. Upon completing troubleshooting procedures, the battalion S6 will assist the user in repairing the automation system. If the support S6 cannot restore the system, the unit will turn in the LRU to the FSC supply platoon.
4	**Software**
	The IMO will use available software troubleshooting tools and utility software. IMOs will also maintain copies of all operating system and application software for reloads when necessary.
5	**Hardware**
	If spare LRUs were provisioned and are on-hand at the FSC, the unit will request and receive a replacement. If spares are not on-hand, the FSC supply platoon will issue a due out to the unit and request a replacement LRU from the BSC SSA.
6	**Network/LAN connectivity**
	If the fault is determined to be in the LAN and the proper tools and/or skill set(s) are not available for the S6 to repair the fault, the G6 will assist the S6 in repairing LAN connectivity problems.
7	**Warranted LRUs**
	Warranted LRUs are managed as repairable exchange using “Off-Line” manual procedures. This is necessary to provide a no cost issue to the unit. Note: The current supply/financial systems interface will not allow for free issue. GCSS-A will remedy this when fielded. For warranted LRUs, the SSA processes a work request to the FRA. Based on the maturity of the theater of operations, the headquarters and supply company (HSC) may process warranted items through the non-divisional maintenance company. For selected items, the FRA is authorized to perform the necessary warranty repair. All others will be returned to the manufacturer. The FRA will return all repaired LRUs to the SSA. The SSA either returns the item to the customer or authorized stockage list (ASL).

Table 3-3. Support Automation-Organic Support Procedures (continued)

8	**Nonwarranted LRUs**
	Nonwarranted systems require coordination between the FSB support operations section, the BSC, and the supporting non-divisional maintenance company. This coordination is required to determine the appropriate repair facility based on the unit's maintenance backlog, personnel, and test equipment available. The SSA will work order the LRU to the appropriate unit for repair. At the BSC/AMC/GMC, maintenance personnel will conduct a technical inspection to verify failure. When a failure exists, the DS maintainer will perform all authorized repair actions to restore the LRU to a serviceable condition. These procedures may involve the use of operating system tools, diagnostic software, and school-taught repair skills. Nonwarranted LRUs are managed as repairable exchange. The repaired LRU is returned to the SSA or returned to the customer for completed work requests. The BSC/AMC and GMC may also evacuate excess workload to the non-divisional maintenance company.
9	**Non-divisional maintenance company**
	The non-divisional maintenance company provides DS maintenance support to units on an area basis. DS maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. The non-divisional maintenance company will return all serviceable LRUs to the customer. Additionally, the unit provides reinforcing and backup DS maintenance to the– • BSC if at the BSA. • AMC and GMC if at the DSA. • SSA if at EAD. • Note: Figure 3-3 shows the general flow of ABCS support for the DSA.
10	**ESSC**
	The ESSC provides warranty/nonwarranty support. Contractor maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. They also provide support in shipping items back to the manufacturer when further repairs are needed. The ESSC returns all serviceable LRUs to the SSA. **Note: Figure 3-7 shows the general flow of support automation (organic). Figure 3-8 shows the general flow of support automation (contract).**

NETWORK DEVICES

Network devices are the hubs, switches, routers, Combat-Service-Support Automation Information Systems Interface (CAISI), and other devices essential for network connectivity. These items are covered in Appendix A. Network devices are currently procured through the CHS-2 program and are maintained under warranty. This maintenance support is

deployable to a theater of operations through CECOM's ESSC. Organic support is limited to fault isolation and replacement at the unit level and the stockage of spares at the DS (SSA) level. Figure 3-9 shows the flow of support for network devices, and Table 3-4 lists the network device support procedures.

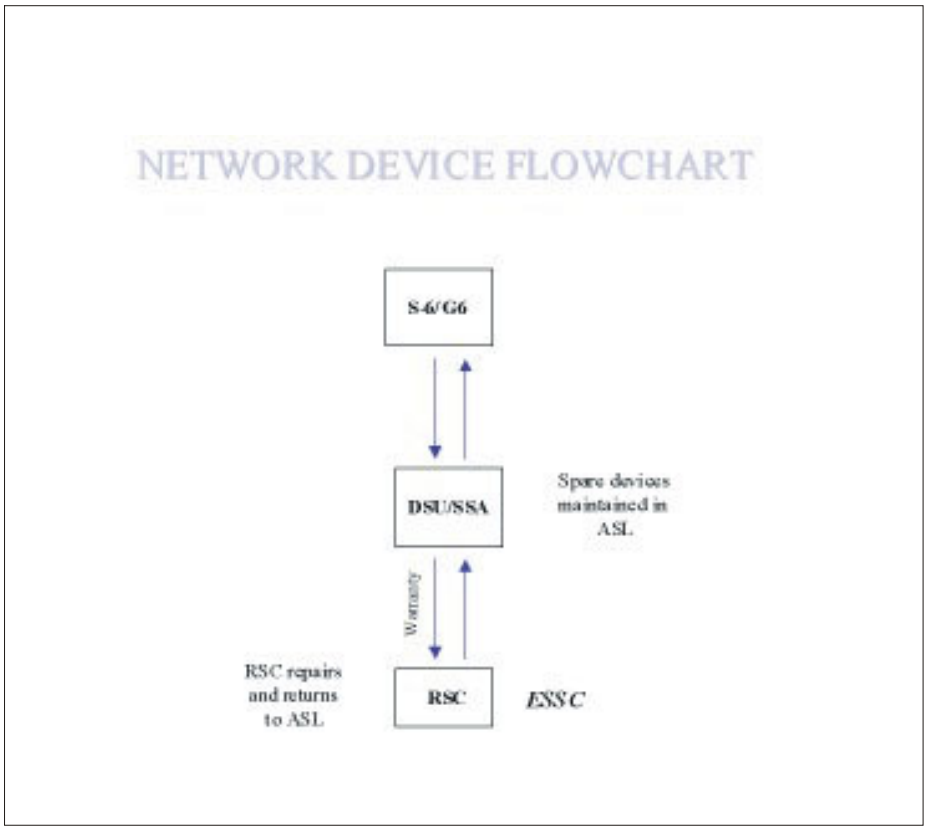

Figure 3-9. Network Devices Support Flowchart

Table 3-4. Network Device Support Procedures

Step	Procedure
1	**The MAU discovers a fault**
	The MAU determines the system to be nonoperational and notifies the MAA/section chief of a system failure. Using diagnostic software and built-in-test equipment, the MAU and MAA will try to determine whether the failure is software, hardware, or network related. For software related problems, the MAU will reload the software, if available, and return the system into operation.
2	**MAA/IMO troubleshoots**
	The MAU/MAA cannot correct the problem or determines the problem to be a network/communications-related failure; he will contact the S6.

Table 3-4. Network Device Support Procedures (continued)

Step	Procedure
3	**The S6 is notified—**
	The S6/G6 troubleshoots and discovers a faulty network device (see step 6). The S6/G6 will immediately request replacement from the supporting SSA. Upon receipt of the serviceable device, the S6/G6 will install the item and attempt to restore the network.
4	**Software**
	If applicable, the S6 will try to reload the operating software in an attempt to get the device operable.
5	**Hardware**
	The S6 identifies the problem to be a malfunctioning LRU and cannot repair it. The S6 will direct the unit to turn the unserviceable LRU into the FSC, or the S6 will consult the G6 for additional assistance in fault isolation and repair. The MAU will request replacement LRUs and turn in the failed LRU through the supporting– • FSC if at the BSA. • SSA if at the DSA/EAD.
6	**Network/LAN connectivity**
	If the fault is determined to be in the LAN and the proper tools and/or skill set(s) are not available for the S6 to repair the fault, the G6 will assist the S6 in repairing LAN connectivity problems.
7	**Warranted LRUs**
	For warranted LRUs, the SSA processes a work request to the appropriate Regional Support Center (RSC). Based on the maturity of the theater of operations, the BSC may process warranted items through the non-divisional maintenance company. Elements of the RSC typically deploy as part of CECOM's ESSC. The RSC will repair all warranted LRUs and return them to the SSA. The SSA returns the item to the user or supply.
8	**Nonwarranted LRUs**
	Nonwarranted systems require coordination between the FSB support operations section, the BSC, and the supporting non-divisional maintenance company. This coordination is required to determine the appropriate repair facility based on the unit's maintenance backlog, personnel, and test equipment available. The SSA will work order the LRU to the appropriate unit for repair. At the BSC/AMC/GMC, maintenance personnel will conduct a technical inspection to verify failure. When a failure exists, the DS maintainer will perform all authorized repair actions to restore the LRU to a serviceable condition. These procedures may involve the use of operating system tools, diagnostic software, and school-taught repair skills. Nonwarranted LRUs are managed as repairable exchange. The repaired LRU is returned to the SSA or returned to the customer for completed work requests. The BSC/AMC and GMC may also evacuate excess workload to the non-divisional maintenance company.

Table 3-4. Network Device Support Procedures (continued)

Step	Procedure
9	**Non-divisional maintenance company**
	The non-divisional maintenance company provides DS maintenance support to units on an area basis. DS maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. The non-divisional maintenance company will return all serviceable LRUs to the customer. Additionally, the unit provides reinforcing and backup DS maintenance to the– • BSC if at the BSA. • AMC and GMC if at the DSA. • SSA if at EAD. • Note: Figure 3-3 shows the general flow of ABCS support for the DSA.
10	**ESSC**
	The ESSC provides warranty/nonwarranty support. Contractor maintainers will perform all authorized repair actions to restore the LRU to a serviceable condition. They also provide support in shipping items back to the manufacturer when further repairs are needed. The ESSC returns all serviceable LRUs to the SSA.

MAINTENANCE MANAGEMENT

Maintenance management procedures for automation systems will be established from unit through support level. The unit level maintenance personnel will use the ULLS program to process all maintenance transactions. DS or system support personnel (CSSAMO) will use the SAMS-1 to control all maintenance actions. The only exception is when the unit ULLS is non functional and requires maintenance. When fielded, the GCSS-A maintenance module will be used to perform both unit and DS maintenance actions. Commanders at all levels will have visibility of all automation failures by implementing maintenance management procedures.

The Army Maintenance Management System (TAMMS) (DA Pam 738-750) describes the forms and records required in performing unit and DS level maintenance. TAMMS will be completed either by manual process or using the automated process described in DA PAM 738-750. However, if the automated systems fail, manual record keeping will be maintained. Regardless of the system in use, the purpose of the TAMMS operation is to create, maintain, and properly dispose of operational, maintenance and equipment historical records in accordance with DA PAM 738-750.

REPAIR PARTS

Units or organizations authorized Shop Stocks, and Combat Spares will comply to AR 710-2 and applicable publications. The Bench stock consists of low dollar repair parts such as nuts, bolts, and associated hardware that will be consumed on a daily basis by operators and maintainers. The Shop stock will consist of DS maintenance repair parts that are demand supported, non-demand supported, and specified initial stockage repair parts for newly introduced end items.

Units will process requests under the automated supply system and IAW AR 710-2.

Automation Support Organizations

CSS for the future Army force (Force XXI) represents a significant change from the current Army of Excellence (AOE) Division. Organizational structures reflect a paradigm shift from a supply-based CSS system to an advanced distribution-based CSS structure. (See Figure 4-1.) This chapter describes some of the new maintenance and supply organizations within the Division and Corps, to include their role in supporting automation systems.

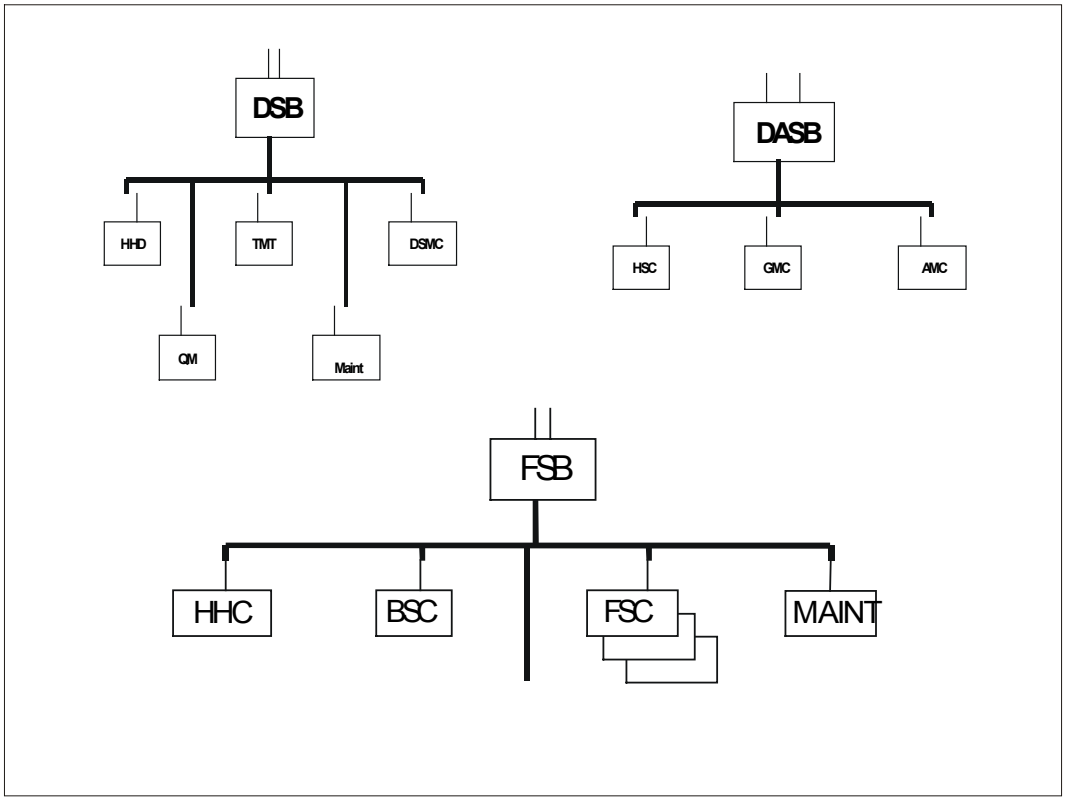

Figure 4-1. Example of New Maintenance and Supply Organizational Structures

DIVISION SUPPORT BATTALION (DSB) QUARTERMASTER (QM) COMPANY

The QM company provides DS supply to division headquarters, DSB, DISCOM headquarters, division artillery (DIVARTY) headquarters, battalion, ADA battalion, MI battalion, Signal battalion, and military police (MP) company. The QM company provides receipt, limited storage, and issue of Classes II, III (bulk) and III (packaged), IV, and IX (less air). It provides receipt and issue of Classes I and VI at the field ration issue point daily and receipt and issue of Class VII at the SSA as required. The Class IX section stocks selected spare LRUs for the various automation systems. The Class IX section work-orders unserviceable LRUs to the appropriate maintenance activity for repair.

AREA MAINTENANCE COMPANY (AMC)

The AMC provides DS maintenance to division troop units, DIVARTY headquarters, and DSB CSS elements operating in the division rear area. (See Figure 4-2.) The AMC also provides DS maintenance support to ADA, MI, Signal, and FA (MLRS) units. Unlike the AOE main support battalion (MSB) maintenance companies, the AMC does not provide backup maintenance support to the forward support battalions. Corps maintenance companies, such as the non-divisional maintenance company, provide this function.

The AMC provides limited repair of automation equipment. Currently, the unit provides DS maintenance of the Advanced Field Artillery Tactical Data System (AFATDS) lightweight computer unit and is projected to repair the FBCB2 system when fielded. Some specific automation support functions include:

- Warranty management.
- Provide DS troubleshooting and repair of selected LRUs.
- Coordinate distribution of warranted LRUs to the ESSC.
- Evacuate excess maintenance to the non-divisional maintenance company.

DIVISION AVIATION SUPPORT BATTALION (DASB) HSC

The HSC consists of a battalion headquarters and a supply company. The battalion headquarters provides C2 and administration support for all organic and attached DASB units. The battalion headquarters plans, directs, and supervises support for the aviation brigade and division cavalry squadron. The supply platoon provides receipt, issue, and storage of Class IX (LRUs and SRUs) for the aviation brigade and division cavalry squadron. The Class IX section stocks selected spare LRUs for the various automation systems. The Class IX section work-orders unserviceable LRUs to the appropriate maintenance activity for repair.

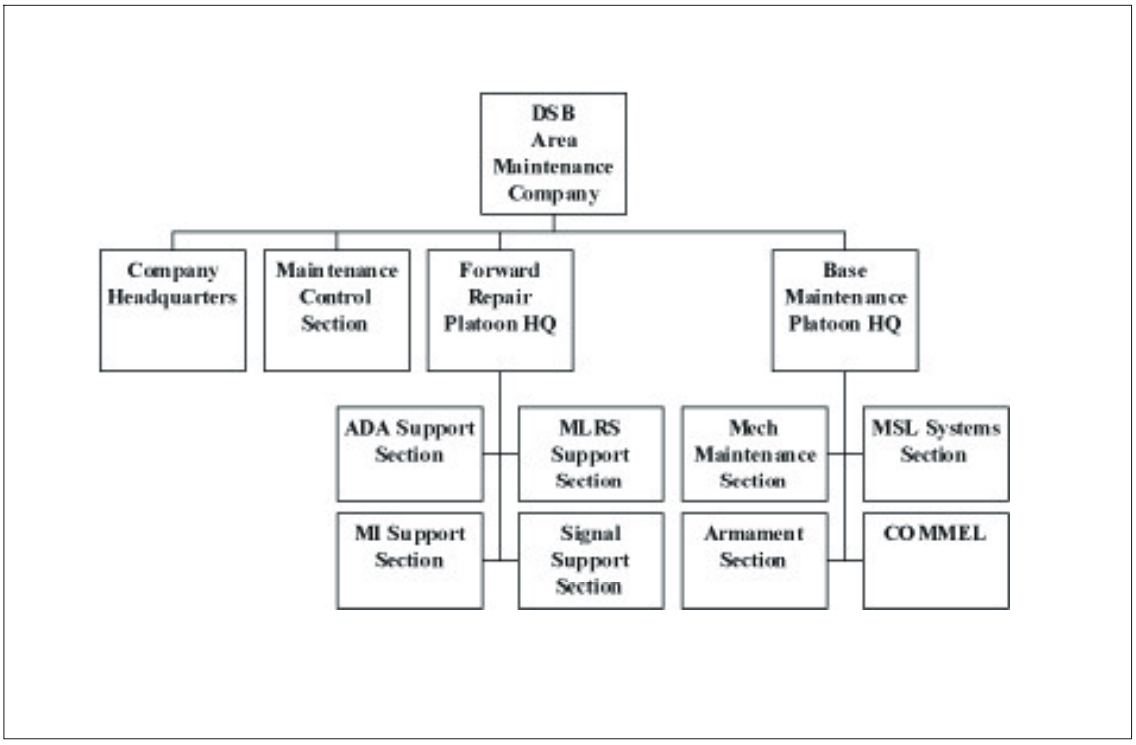

Figure 4-2. AMC Organizational Structure

Ground Maintenance Company (GMC)

The GMC consists of a company headquarters, a battalion maintenance platoon, and a DS maintenance platoon. (See Figure 4-3.) The GMC provides unit maintenance for all DASB non-air items and DS maintenance for all aviation brigade, DASB, and division cavalry non-air items.

The missile support section of the DS maintenance platoon provides repair of selected automation systems. Some specific maintenance management functions include:

- Warranty management.
- Provide DS troubleshooting and repair of selected LRUs.
- Evacuate excess maintenance to the non-divisional maintenance company.

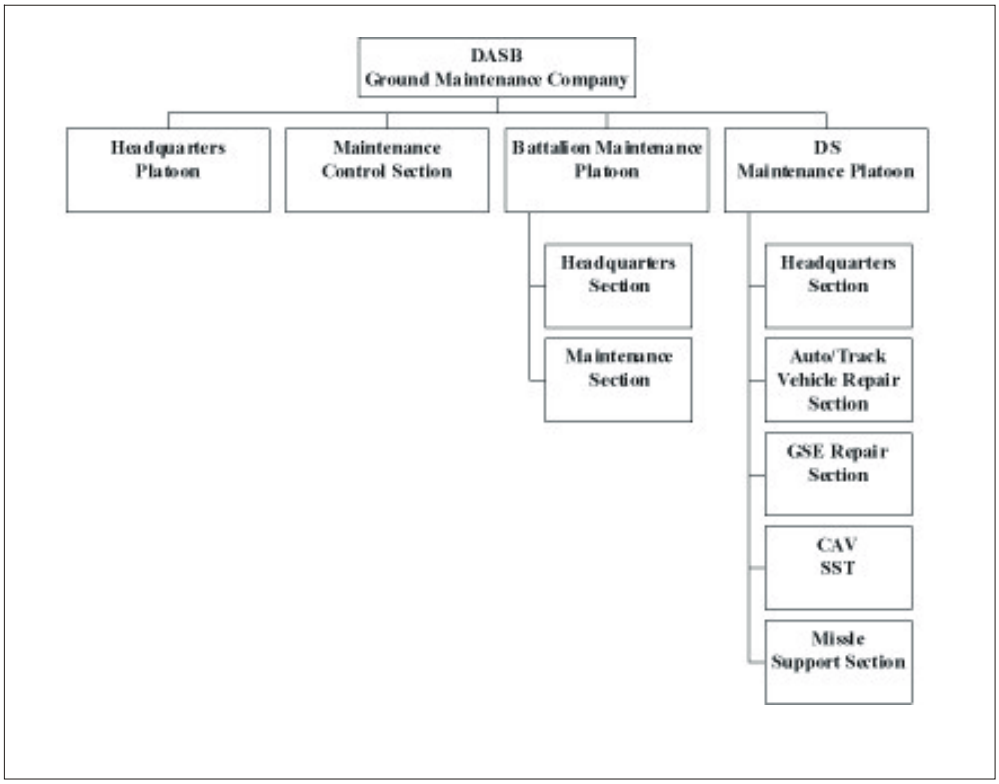

Figure 4-3. GMC Organizational Structure

Base Support Company (BSC)

The BSC is a multifunctional unit that provides CSS to brigade combat teams (BCTs) and divisional units operating within the brigade area. The BSC provides tactical field maintenance to the engineer battalion, brigade headquarters, brigade reconnaissance troop, FSB headquarters, medical company, and BSC. (See Figure 4-4.) The BSC also provides DS base shop, commodity-specific maintenance to the entire BCT. On an area basis, it provides DS maintenance to BCT units within the BSA and limited reinforcing and backup support to the FSCs. The BSC is the first echelon of DS automation maintenance support for the maneuver battalion and division units operating in the brigade rear area. The BSC also provides the brigade a single source for all supply (less Class VIII) and transportation operations. The BSC also maintains Classes II, III (packaged), IV, and IX ASL for the brigade.

The BSC currently performs only limited maintenance of automation equipment. Specific systems include the lightweight computer unit and the FBCB2 system. The majority of new equipment fielded to the first digitized division (FDD) is covered by warranty from the

manufacturer. Spare LRUs may be stocked within the Class IX section of the supply and transportation (S&T) platoon. Unserviceable items are work-ordered to the appropriate maintenance activity (BSC maintenance platoon, non-divisional maintenance company, or the ESSC). Specific automation support functions include:

- Receipt, store, and issue Class IX.
- Maintain repairable exchange of selected LRUs.
- Coordinate distribution of unserviceable LRUs to appropriate repair activity.
- Evacuate excess maintenance to the non-divisional maintenance company.

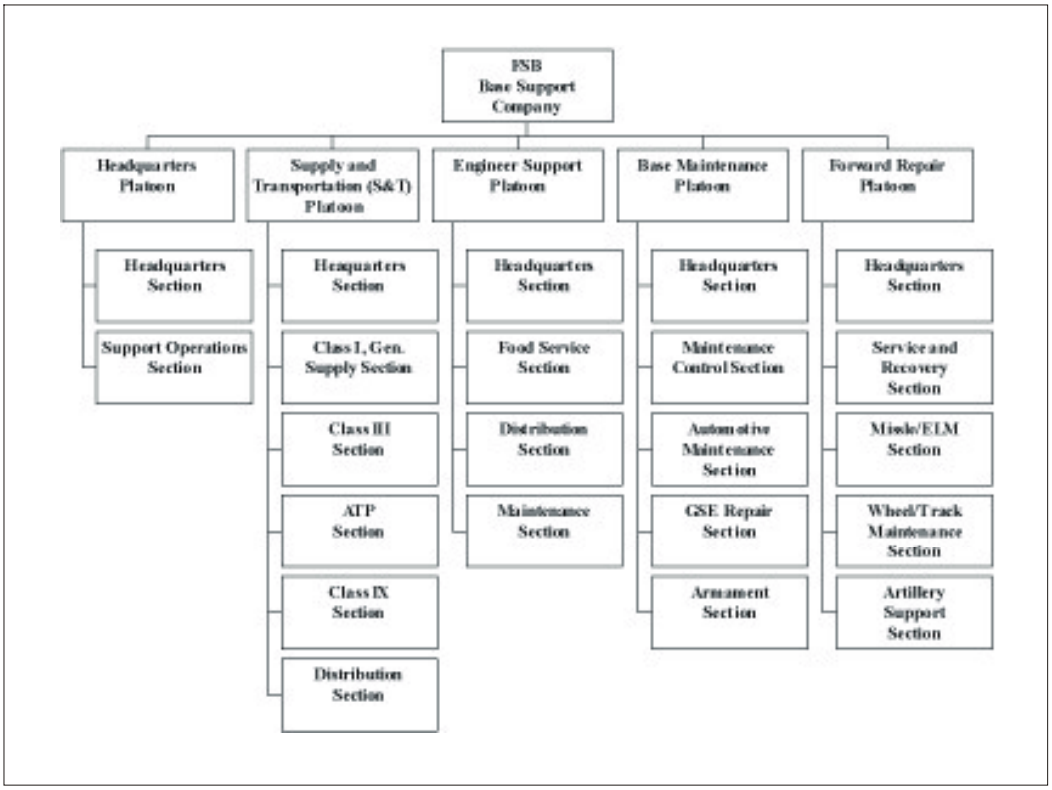

Figure 4-4. BSC Organizational Structure

Forward Support Company (FSC)

The FSC is a multifunctional CSS unit that provides habitual support to a maneuver battalion. The FSC provides unit and DS level maintenance and DS level supply to the supported battalion task force. The FSC requests and issues LRUs for most types of automation. The FSC cannot provide maintenance support for automation equipment. Some specific functions include:

- Request, receive, and issue Classes IX and VII for its supported task force.
- Coordinate distribution of serviceable and unserviceable LRUs from the S6 into the battlefield distribution system.

NON-DIVISIONAL MAINTENANCE COMPANY

The non-divisional maintenance company provides DS maintenance for the division. (See Figure 4-5.) The unit provides repair and return of selected ABCS LRUs and other automation equipment. The supply platoon requests, stores, and issues Class IX, to include SRUs and LRUs. Specific functions include:

- Provide backup DS maintenance support to the division
- Provide DS maintenance support to units on an area basis
- Warranty management
- Provide SAMS-1 support to the corps support group CSSAMO for STAMIS repairs
- Provide DS repair of LRUs
- Maintain repairable exchange of LRUs
- Receive, store, and issue Class IX

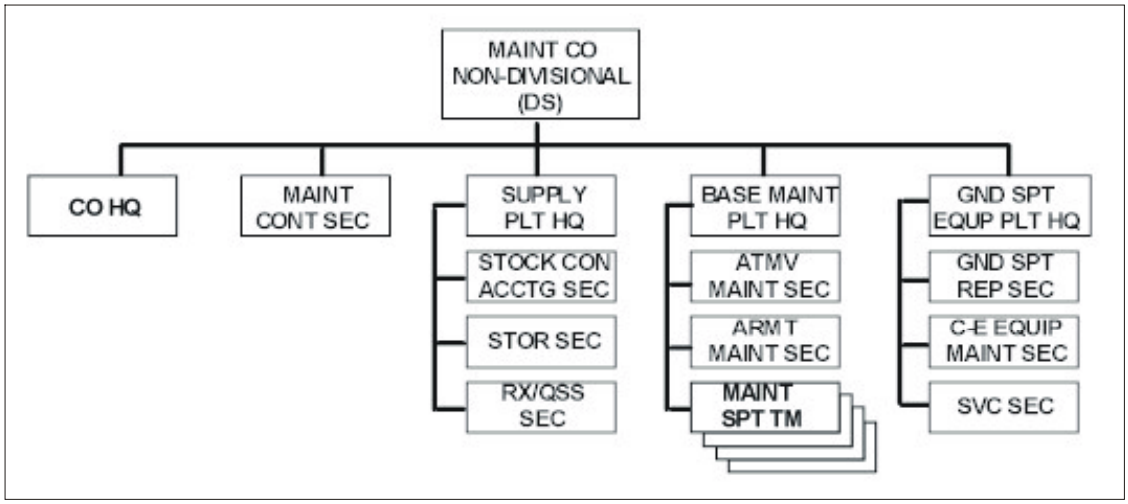

Figure 4-5. Non-Divisional Maintenance Company

Electronic Sustainment Support Center (ESSC)

The ESSCs were established by CECOM as regional organizations to consolidate management of sustainment maintenance and logistics support for communications-electronics (CE) equipment and systems. The ESSC provides one-stop maintenance support for selected Army tactical intelligence and electronic warfare (IEW) and CE equipment, CHS, nonembedded COTS/NDI ADPE, and other COTS/NDI equipment such as nontactical radios, and is expandable to support other electronics equipment repair. The ESSC also provides software logistics support, which is limited to replication, distribution, installation, and training for software upgrades and revisions.

The ESSC supports multiple program executive offices (PEOs) and their associated program/project/product management offices (PMOs) by providing sustainment maintenance and warranty support through one of the ESSC service providers. The ESSC coordinates with the PEOs to ensure appropriate support is in place-fielded systems. The ESSC service providers currently include:

- Tobyhanna Army Depot (TYAD)
- IEW RSC
- Mobile subscriber equipment (MSE) General Dynamics Electronics Systems (GD-ES) RSC

- CECOM Software Engineering Center RSC and Field Service Representatives
- Communications Security Logistics Activity (CSLA) Information Security (INFOSEC) Representatives

Figure 4-6 shows the equipment supported by these service providers.

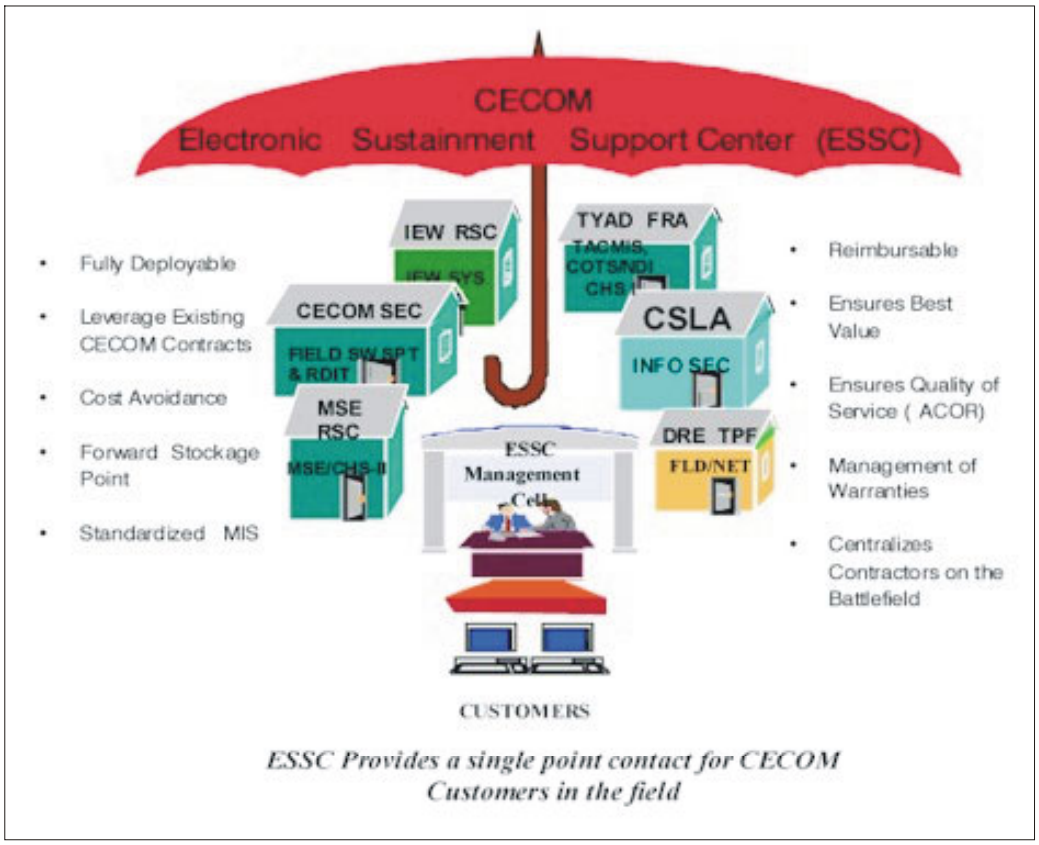

Figure 4-6. Equipment Provided by ESSC Service Providers

Specifically, the ESSC can provide the following functions/services as specified in each individual PMO sustainment plan:

- One-stop shopping for support services.
- Disposition and distribution of failed items to appropriate repair facilities.
- Point of contact/coordination and support for contractor personnel assigned to the area of operations.
- Software replication.
- Distribution of repaired items to the DS units.
- Production control and status.
- Verification of warranty equipment misuse/abuse claims.
- Contingency planning and execution.
- Subject matter expert support for DS units.
- Emergency modification/repair teams as required.
- Field modification of equipment/software when authorized.

- Help desk support.
- Training support assistance by subject matter expert and service provider personnel if available.

One of the efficiencies of the ESSC is its deployability in support of multiple regional conflicts. During deployment, ESSC cells will fully integrate into the logistics support element (LSE). As part of the LSE, ESSC cells will centralize management of contractors performing maintenance and repair on electronics systems and equipment at locations within the area of operations.

CECOM LOGISTICS ASSISTANCE REPRESENTATIVE (LAR)

CECOM provides forward technical and logistics assistance for automation equipment through the network, MSE, and network communications LARs.

The network LAR's responsibilities include:

- CISCO LAN switch
- Integrated system control (ISYSCON).
- Near-Term Digital Radio (NTDR).
- Routers.
- Wireless LAN.
- ABCS.
- CHS-1/2.
- Enhanced Position Location Reporting System (EPLRS).

The network communications LAR's responsibilities include:

- Command and control vehicle.
- FBCB2.
- Single-Channel Ground and Airborne Radio System-Advanced System Improvement Plan (SINCGARS-ASIP).
- Vehicle internal communications (VIC3).
- NTDR.

The MSE LAR's responsibilities include:

- Asynchronous transfer mode small extension node.
- High-speed multiplexer.
- Secure Mobile Antijam Reliable Terminal-Tactical (SMART-T).
- High capacity line-of-sight (HCLOS).
- EPLRS.

CENTRAL TECHNICAL SUPPORT FACILITY (CTSF)

The CTSF is a PEO for the command, control, and communications (C3) system organization located at Fort Hood, Texas, which provides three major services for ABCS and the FDD. A software-testing element provides integration, replication, support, configuration management, distribution, testing, and interoperability certification for the ABCS and CSS AIS applications. A training element provides ABCS collective training development and instruction and hosts the AIS training teams and various contractor FDD training programs. An adjacent installation facility installs ABCS platforms for the FDD and other digital units.

Networks and Automation Systems

Brief descriptions of the supported networks and automation systems are covered in this appendix.

WARFIGHTER INFORMATION NETWORK (WIN)

WIN is an integrated command, control, communications, and computers (C4) network comprised of commercially-based high technology communications network systems. It is designed to enable the gaining of information dominance by increasing the security, capacity, and velocity (speed of service to the user) of information distribution throughout the battlespace. A common sense mix of terrestrial and satellite communications is required for a robust ABCS. WIN will support the warfighter in the 21st century with the means to provide information services from the sustaining base to deployed units worldwide.

WARFIGHTER INFORMATION NETWORK-TACTICAL (WIN-T)

The WIN-T portion of WIN is focused on the terrestrial (nonsatellite) transmission and networking segment of the WIN. The terrestrial transport system is the backbone infrastructure of the WIN architecture as well as the LAN in support of the ABCS capable TOC (ABCS LAN). It provides simultaneous secure voice, data, imagery, and video communications services.

TACTICAL INTERNET (TI)

The TI will enhance warfighter operations by providing an improved, integrated data communications network for mobile users. The TI passes command, control, communications, computers, and intelligence (C4I) information, extending tactical automation to the soldier/weapons platform. The TI will focus on brigade and below to provide the parameters in defining a tactical automated data communications network.

ABCS

ABCS assists the commander in exercising C2 of available forces in the accomplishment of a mission. It allows him to “see and understand” his battlespace and gain dominant situational awareness on the battlefield. ABCS provides the commander with immediate access to situational updates and execution information and allows him to transmit situational understanding and execution from his location on the battlefield.

ABCS is the integration of fielded, developmental, and AISs and communications employed in both training and tactical environments, in both developed and undeveloped theaters, and in fixed installations and mobile facilities. Additionally, the subsystems will interoperate with other Department of Defense and commercial communications systems, including satellite communications systems, Defense Data Network (DDN), Defense Information System Network (DISN), and the Automatic Digital Network (ADN) implementations of the Defense Messaging System (DMS).

ABCS components include the–

- Advanced Field Artillery Tactical Data System (AFATDS)
- Maneuver Control System (MCS).
- Air and Missile Defense Planning and Control System (AMDPCS).
- All Source Analysis System-Remote Workstation (ASAS-RWS).
- Global Command and Control System – Army (GCCS-A).
- Combat Service Support Command System (CSSCS)
- Force XXI Battle Command Brigade and Below (FBCB2).
- Tactical Air Intelligence System (TAIS)

Additionally, the following supporting systems and functions are enablers and shall provide integral support to the overall communications requirements (see Figure A-1) for ABCS.

- Army Airspace Command and Control (A2C2) Tactical Airspace Information System (TAIS).
- Digital Topographic Support System (DTSS).
- Integrated Meteorological and Environmental Terrain System (IMETS).
- Warfighter Information Network (WIN).
- Tactical Internet (TI).
- ISYSCON.

Maneuver Control System (MCS)

MCS is the primary battle command source, providing the common operational picture, decision aids, and overlay capabilities to support the tactical commander and the staff via interface with the force level information database populated from other AISs. MCS provides the functional common applications necessary to access and manipulate the Joint Common Database (JCDB). MCS will satisfy information requirements for a specific operation; track resources; display situational awareness; effect timely control of current combat operations (offense, defense, stability, and support); and effectively develop and distribute plans, orders, and estimates in support of future operations. It will support the military decision-making process. MCS will be deployed from corps to the maneuver battalions.

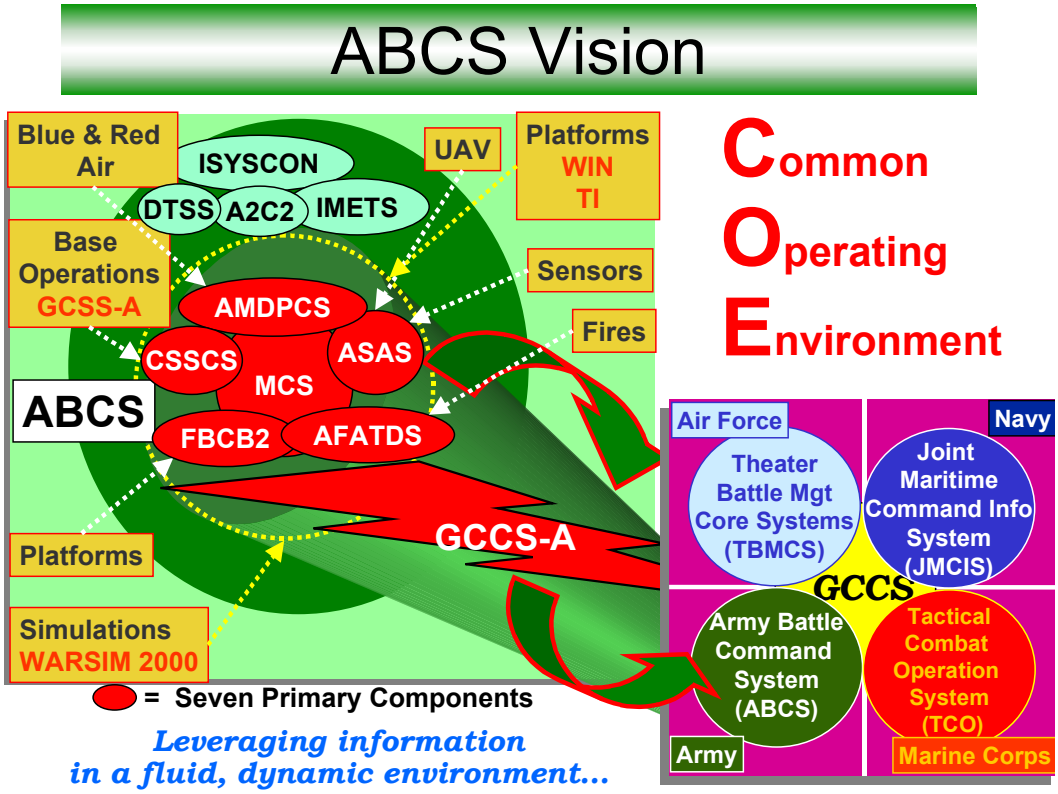

Figure A-1. Current ABCS

Advanced Field Artillery Tactical Data System (AFATDS)

AFATDS provides automated decision support for the fire support (FS) functional subsystem, to include joint and combined fires (that is naval gunfire, close air support). AFATDS provides a fully integrated FS C2 system, giving the FS coordinator (FSCOORD) automated support for the planning, coordination, control, and execution of close support, counter fire, interdiction, and air defense suppression fires. AFATDS performs all of the FS operational functions, to include automated allocation and distribution of fires based on target value analysis. AFATDS will be deployed from echelons above corps (EAC) to the firing platoons. AFATDS provides FS overlay information to the ABCS common database. AFATDS will interoperate with the United States Air Force, Theatre Maritime Battle Management Core System, and the United States Navy/United States Marine Corps Joint Maritime Combat Information System. AFATDS will also interoperate with the FS C2 systems with allied countries, including the United Kingdom, Germany, and France.

AMDPCS FORWARD AREA

AMDPCS integrates air defense fire units, sensors, and C2 centers into a coherent system that can defeat/deny the aerial threat (unmanned aerial vehicles, helicopters, fixed wing, and so forth). AMDPCS provides for automated, seamless C2 and Force XXI vertical and horizontal interoperability with joint and coalition forces for US Army air and missile defense (AMD) units. The system provides CHS modules at all echelons of command, which will provide for highly effective employment of Army AMD weapon systems as part of the joint force. AMDPCS provides the third dimension situational awareness component of the common operational picture. Initially, the AMD-workstation

(AMD-WS) will provide elements from EAC to battalion the capability to track the AMD battle force operations.

ASAS-RWS

The ASAS-RWS is the IEW component from EAC to battalion. It is a mobile, tactically deployable, computer-assisted IEW processing, analysis, reporting, and technical control system. The ASAS-RWS receives and rapidly processes large volumes of combat information and sensor reports from all sources to provide timely and accurate targeting information, intelligence products, and threat alerts. It consists of evolutionary modules that perform system operations management; system security; collection management; intelligence processing and reporting; high value/high payoff target processing and nominations; and communications processing and interfacing. The ASAS-RWS provides automated support to the doctrinal functions of intelligence staff officers (G2/S2) from EAC through battalion, including Special Operations Forces. It also operates as the technical control portion of the intelligence node of ABCS to provide current IEW and enemy situation information to the JCDB for access and use by ABCS users. The ASAS-RWS produces the enemy situation portion of the common operational picture of the battlefield disseminated via the ABCS network.

CSSCS

The CSSCS provides automated CSS information to maintenance, medical, personnel, classes of supply, personnel service support and movements to CSS, maneuver and theater commanders, and logistic and special staffs. Critical resource data is drawn from both manual resources and STAMIS at each echelon, which will evolve to the GCSS-A (the unclassified logistics wholesale/resale business-end connectivity). The CSSCS processes, analyzes, and integrates resource information to support evaluation of current and projected force sustainment capabilities. The chaplaincy is an active participant in CSSCS and will be included in the development of CSS services. The CSSCS provides CSS information for the commanders and staff and will be deployed from EAC to battalion.

FBCB2

The FBCB2 is a suite of digitally interoperable applications and platform hardware that provide on-the-move, real-time and near-real-time situational awareness and C2 information to combat, combat support, and CSS leaders from brigade to the platform and soldier level. The FBCB2 is a mission essential sub-element and a key component of ABCS. The FBCB2 will feed the ABCS common database with automated positional friendly information and current tactical battlefield geometry for friendly and known/suspected enemy forces. The goal is to field FBCB2 to the tank and Bradley-fighting vehicle and other platforms with a common look and feel screen. CHS design will facilitate training and standard operating procedures.

A2C2 TAIS

The TAIS provides A2C2 functionality. Full airspace C2 is not yet resident within ABCS, and the TAIS is migrating to meet this requirement.

DTSS

The DTSS is an automated system that provides tactical and operational commanders with geo-spatial information to support terrain visualization. The DTSS is the terrain analysis tool that provides geo-spatial information and special mission-specific products to ABCS for battlespace operations supporting EAC to brigade and platform level. The DTSS collects source material, manages digital terrain databases, and distributes material through a geo-spatial digital data storage device. The DTSS Geographic

Information System (GIS) and imagery analysis software components allow the analyst to density, manipulate, analyze, and produce standard and special topographic products for the battle commander. National and in-theater sources will provide new and enriched data to update the geo-spatial database. The DTSS uses established ABCS tactical and satellite communications means.

IMETS

IMETS is an AIS that can display and analyze weather products and provide general weather forecasting, weather warnings, and weather effects analysis for the commander and his staff to support mission planning and execution.

ISYSCON

ISYSCON provides an automated management and synchronization of multiple tactical C3 systems. ISYSCON is used at theater, EAC, corps, and division down to brigade and below. It provides automated network management assistance for network planning and engineering, battlefield spectrum management, Signal C2, WAN, and COMSEC. In addition, ISYSCON provides LAN management capabilities to monitor and maintain ABCS/STAMIS connectivity and communications services in the TOC.

GCCS-A

The GCCS-A is the Army link for ABCS to the GCCS. The GCCS-A will provide a suite of modular applications and information and decision support to Army strategic/operational/theater level planning and operational/theater operations and sustainment. The GCCS-A will support the apportionment, allocation, logistical support, and deployment of Army forces to the combatant commands. Functionality includes force tracking, host nation and civil affairs support, theater air defense, targeting, psychological operations, C2, logistics, medical, provost marshal, counter-drug, and personnel status. The GCCS-A will be deployed from theater EAC elements to division.

STAMIS

Each STAMIS is different; each has requirements governing specific site location and operations. STAMIS software is mission critical and must be accommodated before all other automation issues. It is the essential data that resupplies, requisitions, and repairs the Army. Many STAMIS software packages feed data to the Joint Chief of Staff (JCS) level and are time critical in delivery and execution. STAMIS systems must not be interfered with and must not fail because of misuse of automation assets. The direct result of STAMIS failure will manifest itself on the unit's ability to conduct its wartime mission and an undesirable reflection on the unit status report. The logistical STAMIS will be replaced by the GCSS-A.

DEPARTMENT OF THE ARMY MOVEMENT MANAGEMENT SYSTEM-REDESIGN (DAMMS-R)

DAMMS-R provides automation support for transportation staffs and organizations within a tactical theater of operations. It also supports transportation units within the continental United States (CONUS). DAMMS-R supports the Army's strategic mobility programs and is a vital link in the maintenance of intransit visibility over units, personnel, and materiel in the deployment and distribution pipeline. The system is divided functionally into seven subsystems or modules.

- System management subsystem.
- Mode subsystem.
- Movement control team operations subsystem.

- Highway regulation subsystem.
- Convoy planning subsystem.
- Operational movement programming subsystem.
- Transportation addressing subsystem.

The Transportation Coordinators Automated Information for Movements System-II (TCAIMS-II) will replace the DAMMS-R.

SAAS-MOD

The SAAS-MOD will provide centralized information management to support ammunition management functions on the battlefield and in CONUS, overseas, and within the major commands.

SAMS

SAMS increases the productivity of maintenance shops and provides commanders with accurate and timely maintenance management information. It provides visibility of inoperative equipment and required repair parts, selected maintenance, equipment readiness, and equipment performance reports. SAMS also provides completed work order data to the Logistics Support Activity (LOGSA) for equipment performance and other analyses. It further manages maintenance actions, workloads, and resources.

SAMS can automatically process DS/GS maintenance shop production functions, maintenance control work orders, and key supply functions previously performed manually. Requisitions are prepared automatically and automatic status is received from the SARSS-1. SAMS operates in the DS/GS maintenance and/or aviation intermediate maintenance (AVIM) activity, FSB, DSB, DASB, corps support battalion (CSB), ASG, and the Materiel Management Center (MMC) within division, corps, and EAC environments. SAMS consists of SAMS-1, SAMS-2, and SAMS-Installation/Table(s) of Distribution and Allowances (I/TDA).

SAMS-1 automates shop production functions and maintenance control records, maintains shop supplies, and requests repair parts. It receives maintenance data from the battalion maintenance section's ULLS.

SAMS-2 provides field commanders with selected maintenance, equipment readiness, and equipment performance reports. It also provides readiness data and life-cycle management data to the Army Materiel Command (LOGSA) databases.

SAMS-I/TDA is the nontactical installation-based application that provides standard automated maintenance operations management information to I/TDA DS and GS levels.

SARSS

SARSS is a multiechelon supply management and stock control system designed to operate in tactical and garrison environments. It supports the ULLS-G, ULLS-A, ULLS-S4, SAMS-1, SPBS-R STAMIS, nonautomated customers, and the split operations concept. SARSS is fully integrated from the user through theater Army level. It can support worldwide deployment of combat forces in various scenarios and areas of operations, ranging from low to mid to high intensity conflict, including smaller-scale contingencies. SARSS is employed in DS and GS Units, SSAs, division MMC, armored cavalry regiment MMC, and separate combat brigade MMC throughout the Army. The Automated Information Technology (AIT) source data automation is provided through use of radio frequency tags, fixed and handheld radio frequency interrogation devices, optical laser card readers/writers, and bar-code readers.

SIDPERS

SIDPERS-3 brings real-time military personnel management and strength accounting processing to the desktop. It is found within the Personnel Services battalion at the division, corps, and theater levels. The system also is found at the unit level (S1/G1) from battalion through corps. The system consists of relational database application software written in Ada and a hardware suite. The hardware architecture is a host-based design with a terminal server as the hub, which includes the database. Up to four remote PCs can connect to the terminal server to access the database and to run office automation applications while it is not performing SIDPERS-3 functions.

SIDPERS-3 provides many benefits. It reduces transaction-processing time between the field and Headquarters, Department of the Army from days to hours, quickly giving commanders more accurate information. System input edits, and help screens enable the user to increase productivity and reduce errors. Additional enhancements are the ability to produce an officer or enlisted record brief at any level down to battalion and separate unit along with a fully automated promotion module.

SPBS-R

The SPBS-R provides on-line management information and automated reporting procedures for the property book officer and produces updated company-level hand receipts when needed. It also provides automated interfaces with SSAs for request and receipt of equipment, Continuing Balance System-Expanded (CBS-X) for worldwide asset reporting, LOGSA for total asset visibility (TAV), catalog updates, unique item tracking (UIT) for weapon serial number tracking, and ARMS for NDI computer serial number tracking and warranty information.

The SPBS-R is used in brigade, division, corps, Army area, and theater of operations environments. The SPBS-R can automatically process Class II and Class IV, Class III (packaged), and Class VII supply requirements to the SARSS and the basic load Class V requests submitted to the SAAS-4.

TAMMIS

TAMMIS consists of six subsystems that support logistics and patient administration functions. The subsystems that support logistics are Medical Supply (MEDSUP), Medical Assemblage Management (MEDASM), and Medical Maintenance (MEDMNT). The subsystems that support patient administration are Medical Regulating (MEDREG), Medical Patient Accounting and Reporting (MEDPAR), and MEDPAR Command and Control (MEDPAR-CC). TAMMIS can interface with other Department of Defense management information systems and programs such as the Defense Medical Regulating Information System (DMRIS), SIDPERS-3, Prime Vendor Program, Standard Financial System (STANFINS), and many, many more. TAMMIS automates communications by setting up a transmission schedule to remote locations and automating retransmissions. TAMMIS can relay information between units in various ways. The preferred methods use the tactical terminal adapter (TTA) or LAN. Both methods rely on the MSE military communications system. Because communications cannot be assured in wartime, units can also pass information by standard telephone lines, DDN, or an international maritime satellite (INMARSAT) using a commercial modem; over a stand-alone LAN (without MSE); and by floppy diskette or tape delivered by a courier. In the near future, we hope to also be able to pass data using the high frequency radio. All methods preclude re-entering data at the receiving unit.

Medical Communications for Combat Casualty Care (MC4)

Medical Communications for Combat Casualty Care (MC4) is a family of systems hardware program that meets the Army's tactical (combat casualty care) medical needs. It is responsible for fielding and life cycle support for nine (objective) Joint Theater Medical

Information Program medical software system applications. It will automate and link these nine medical applications, while enhancing digital communications, and promoting medical situational awareness to command and control structures, through the use of existing and emerging COTS/GOTS technologies. It will also provide visibility of deployed medial forces and casualties as well as provide an accurate and timely means for documenting healthcare from the point of care to a centralized database in the theater of operations. This centralized database will link healthcare providers, medical diagnostic systems, evacuation information, and medical logistics management to all levels of the Army's Composite Health Care System (CHCS). This MC4 TMIP-A system will be accomplished by integration of fully integrated, validated and approved software provided by the joint Theater Medical Information Program (TMIP).

The ten MC4 TMIP-A software applications are the –

- Defense Medical Logistical Support System – Assemblage Management (DMLSS-AM) Medical resupply, logistics inventory management, assemble management & product ID/storage
- Personal information Carrier (PIC) – Store and transport personal medical information
- Defense Blood Standard System (DBSS) Blood products inventory, requisitioning, movement, tracking, & storage
- Local Data Base (LDB) - Medical records consolidation & collection
- Lower Echelon Reporting and Surveillance Module (LERSM) Patient tracing, evacuation, visibility, status reporting & treatment
- Medial Reference Component (MRC) Medical reference library
- Patient Encounter Module (PEM) Encounter data collection
- Immunization Tracking System (ITS) Record/report immunizations
- Health Surveys (HS) Post deployment assessment

ULLS

ULLS provides tactical line companies and supporting CSS companies the capability to automate logistics at the unit level. The ULLS application software operates on a standard computer centrally procured NDI computer platforms, and peripheral devices. Following are the different ULLS applications:

ULLS-A

The ULLS-A is located in all aviation units. It performs those functions for aviation that ULLS-G performs for ground units.

ULLS-G

The ULLS-G is located at any unit that has an organizational maintenance facility. It automates vehicle dispatching, PLL management, and TAMMS. The ULLS-G interfaces with the SARSS-1, SAMS-1, IVIS Inter-Vehicle Information System (IVIS), vehicle sensors, and ULLS-S4. The AIT interrogator connects directly to the ULLS-G. The ULLS-G links to the wholesale supply system through the objective supply capability (OSC).

ULLS S4

The ULLS-S4 is located at unit level supply rooms, as well as battalion and brigade level S4 staff sections. The ULLS-S4 automates the supply property requisitioning/document register process, hand/subhand receipts, component, budget, and logistical planning activities at the unit supply, battalion, and brigade S4 levels. It also receives and

produces the Army Materiel Status System (AMSS) reports generated by the ULLS-G/A systems or by another ULLS-S4. The ULLS-S4 interfaces with the SPBS-R, ULLS-G, and ULLS-A (for budget and AMSS data transferring); the SAAS; the SARSS-Objective (SARSS-O) at the DS level; the OSC SARSS gateway; and the CSSCS.

GCSS-A

The GCSS-A will be the Army's AIS to modernize and integrate the capabilities of the existing logistics STAMIS. These capabilities will include supply, property, ammunition, and maintenance functions (less medical) with significant enhancements. The principal logistics STAMIS systems to integrate include the ULLS, SARSS, SPBS-R, SAAS, and SAMS.

The six GCSS-A modules are the–

- Modernized supply and property module that integrates supply operations and property accountability in all units.
- Modernized maintenance module that integrates maintenance operations (ground, aviation, and water equipment) at all maintenance levels.
- Modernized ammunition supply point module that integrates Class V management and operations.
- Modernized SSA module that integrates the supply management and operations at SSAs and storage sites.
- Modernized and integrated materiel management module that integrates supply, property, ammunition, and maintenance management in all materiel management organizations.
- Management module that integrates information from multifunctional CSS data sources and allows for data exchange with other GCSS-A modules and external AISs.

In addition to the replacement of legacy system functions of the logistics STAMIS systems above, a variety of functional enhancements are planned for incremental block development. These enhancements provide automation tools and functional applications that support other CSS mission requirements, including:

- Food service operations.
- Troop issue subsistence operations.
- Legal affairs and assistance operations.
- Religious support and unit ministry team operations.
- Mortuary and memorial affairs operations
- Class III bulk accountability and distribution.
- Central issue facility operations and accounting for organizational clothing and individual equipment.
- Clothing issue point operations.
- Water supply operations.
- Finance unit operations to include the Installation Finance Office.
- Arms room and tool room operations.
- Forward maintenance support team, contact team, and equipment recovery team operations.

The GCSS-A will establish interfaces so that users can gain access to information and exchange operational data in the areas of personnel, medical, finance, transportation, training, unit administration, and other CSS functional areas. Some examples of these interfaces include–

- SIDPERS.
- The Defense Integrated Manpower Human Resources System (DIMHRS).
- The Tactical Personnel System (TPS).
- The Defense Medical Logistics Standard System (DMLSS).
- The Defense Casualty Information Processing System (DCIPS).
- TCAIMS-II.
- The Battlefield Company Information System (BCIS).

The GCSS-A will also establish interfaces to weapons system data collectors and automated diagnostic and prognostic systems such as the voice activated data recorder (VADR), Soldier Portable On-System Repair Tool (SPORT), Failure Analysis and Maintenance Planning System (FAMPS), Health Usage and Monitoring System (HUMS), Longbow Integrated Maintenance Support System (LIMSS), and the digital source collector (DSC). Selected data from weapons system processors and automated diagnostic tools will be transported where needed to support fleet management, trend analysis, and other purposes.

Tier 1 – Initial Operational Capability (Integration and Modernization)

In this tier, an initial operational capability (IOC) will be developed through incremental integration and modernization of current tactical logistics STAMIS systems. The principal ones to integrate will include the ULLS, SARSS, SPBS, SAAS, and SAMS. The six GCSS-A modules will be the products of this integration.

All components of the GCSS-A must communicate flexibly. The system will be designed to take advantage of all available methods of communications, including tactical packet networks, circuit switch networks, wireless networks, the DISN, telephone networks, and strategic communications capabilities. The sneaker net will be used only as necessary to transfer information on removable media.

Tier 2 – Enhanced Operational Capability (Wholesale and Retail Integration)

This tier will enhance the IOC provided in Tier 1 by the redesign of CSS business practices to include integrating wholesale CSS functionality. Design and development will capitalize on advanced technology, electronic data interchange, advanced warfighting experiments, emerging battlefield distribution concepts, Force XXI initiatives, decision support tools, interfaces with wholesale-automated systems, and integration of the Army Total Asset Visibility System. The initial focus is on logistics modernization (LOG MOD), which is intended to privatize the functions of the current wholesale Standard Depot System **(**SDS) and the Commodity Command Standard System (CCSS).

Tier 3 – Full Operational Capability (Joint Integration)

This tier will implement all required interfaces with automated systems in the joint community, national sustaining base, and applicable allied systems. Access will be available to CSS data sources, and complete interoperability will be achieved when operating in the open system environment. This tier will provide a seamless, integrated, modular, interactive, and interoperable CSS automated system for the total Army.

TCAIMS-II

The TCAIMS-II, a joint system, will be an aggregation of the US Air Force Cargo Movement Operations System (CMOS), the USA Transportation Coordinator Automated Command and Control Information System (TCACCIS) and DAMMS-R, the Marine Air-Ground Task Force (MAGTF) Deployment Support System (MDSS), and the US Marine Corps TCAIMS, possibly the air load module (ALM), and the Integrated Computerized Deployment System (ICODES). The TCAIMS-II is part of the reengineering of the Defense Transportation System (DTS). It will empower the user to–

- Build automated unit equipment lists and deployment equipment lists from standard retail supply and personnel systems.
- Plan convoys and request convoy clearances.
- Request transportation support from all modes.
- Conduct load (air/sea/rail) planning.
- Manage mode operations.
- Pass information to the strategic transportation systems.
- Provide enhanced unit/sustainment intransit visibility data and total asset visibility data.
- Execute the day-to-day operations of the Installation Transportation Office/Traffic Management Office (ITO/TMO).

SUPPORT AUTOMATION

Automation has become an integral part of tactical operations. Computers are used in nearly every section of a unit from the motor pool to the orderly room. Contributing to this expansion is the Department of Defense trend towards a paperless environment. Currently, the Army is in the process of converting all paper technical manuals (-20 level and higher) to CD-ROM. The Army is also undertaking a major diagnostic improvement effort, focused on modernizing its aging, cumbersome test, measurement, and diagnostic equipment (TMDE).

Headquarters, Department of the Army will likely not restrict units from purchasing support automation for mission needs. In fact, CTA 50-909 allows commanders to purchase computers to support mission requirements. This could produce a tremendous maintenance problem for many units. As a result, major commands should consider establishing policy that regulates the types and quantity of support automation equipment units deploy with. This procedure will assist logisticians in developing support plans and priorities for automation equipment. Additionally, it may prevent overwhelming the supply and maintenance systems.

OFFICE AUTOMATION

Office automation includes computers and ADPE used only to support a unit's garrison mission. These items are not used in the tactical environment. Office automation deployed in a tactical environment is the sole and deliberate decision of the unit commander. This decision may impact on readiness if the office automation system fails in a tactical environment and the commander has not made unit level maintenance coordination and provisioning to sustain these items. The commander is responsible for repair or nonuse of these items if deployed in a tactical environment. Office automation includes desktop or laptop computers and peripheral equipment. These computers are required for unit administration and have become essential for mission accomplishment.

ELECTRONIC TECHNICAL MANUAL (ETM) READERS

ETM readers are laptop computers with built-in CD-ROM drives. They are fielded to support maintenance operations in the digital age. ETM readers provide operators and mechanics a lightweight, portable tool for CSS operations. They allow mechanics to easily access troubleshooting procedures and repair parts information while performing maintenance operations. In the future, these devices will also interface with the logistics STAMIS (GCSS-A). The Logistics Integration Agency is also experimenting with wireless alternatives for maintenance operations.

COMPUTER-BASED TMDE

Computer-based TMDE is rapidly replacing the Army's aging inventory of analog test equipment. The SPORT is a Pentium processor-based portable computer that replaces the current contact test set and the Simplified Test Equipment-Internal Combustion Engine (STE-ICE). It is an on-system tester designed to augment the built-in test/built-in test equipment capability of Army systems. The SPORT comes equipped with a built-in CD-ROM reader, which allows it to serve as a delivery device for ETMs and interactive ETMs (IETM), and a software loader verifier. The SPORT will be an integral part of every unit motor pool within the Army.

COMMUNICATIONS SYSTEMS SUPPORTING ABCS AND STAMIS

Army communications are divided into four systems: the Army Data Distribution Center (ADDS), Area-Common User System (ACUS), Combat Net Radio (CNR), and Broadcast.

ADDS

ADDS is an integrated C3 system providing near-real-time transmission capabilities to support low to medium volume data networks. ADDS automatically relays information from the origin to the destination transparent to the user. EPLRS and JTIDS are subsystems of ADDS.

ACUS

The ACUS is a communications system made up of network node switching centers connected primarily by LOS multichannel radios and tactical satellites (TACSATs). Army ACUS networks are the Tri-Service Tactical Communications (TRI-TAC) at EAC and MSE at echelons corps and below (ECB). The ACUS provides a multiuser, common-user area system for high-volume voice and data communications.

MSE

The MSE system is the primary ACUS configuration for ECB. MSE forms a network that covers the area occupied by unit subscribers. For a division, the grid is made up of four to six centralized node centers (NCs), which make up the hub or backbone of the network. Throughout the maneuver area, subscribers connect to SENs/large extension nodes (LENs) by radio or wire. These extension nodes serve as local call switching centers and provide access to the network by connecting to the NCs.

The MSE system provides both voice and data communications on an automatic, discrete addressed, fixed-directory basis using flood search routing. The system supports both wire and mobile subscribers.

Tactical Packet Network (TPN)

The TPN is overlaid on the MSE network and uses existing trunks exclusively for data transmission. Users can connect computers and LANs to the TPN from their command posts. Rather than using a direct end-to-end connection, which ties up an entire trunk,

the TPN breaks up the data into “packets” and routes them along their most efficient path to their destination. When all packets arrive, the receiving packet switch reassembles the data and sends it to its destination.

CNR

The CNR is a system of systems consisting of SINCGARS, a TACSAT communications system, and high frequency radios. CNRs are the primary means of communications in maneuver units. To support the commander, units use these radios in networks such as command, administrative/logistical, and intelligence/operations.

BROADCAST

Broadcast communications systems use technology similar to commercial radio stations. Transmit-only stations send information to high frequency radio systems, satellites, unmanned aerial vehicles (UAVs), or other means. Weather, intelligence, and position location/navigation (POS/NAV) information are support derived from the broadcast system.

LAN

A LAN is a data communications network that interconnects digital devices and other peripherals. These are linked and distributed over a localized area for communicating between computers and sharing resources. Two or more computers linked by software and connected by cable are considered a LAN. A LAN includes–

- Digital devices (computers, scanners, printers, and other peripherals).
- A communications medium that exchanges data from one device to another.
- Network adapters that provide devices with an interface to the communications medium.

Digital systems within a command post are normally connected on a LAN (several command posts are so large that they comprise several LANs). Tactical LANs can be configured as switch-based or router-based architecture interconnecting the various systems. Routers on the LAN allow addressees to change as needed for jump and/or split operations. The LAN manager physically establishes, connects, and maintains the operation and troubleshoots the LAN. Figure A-2 shows a generic tactical LAN configuration. The specific LAN interfaces determine the number of devices used per LAN segment. LANs usually have a connector (port) to which an adapter is connected, and then a coaxial cable is connected between “tee” connectors on this port to form the data bus. LAN length should not exceed 600 feet.

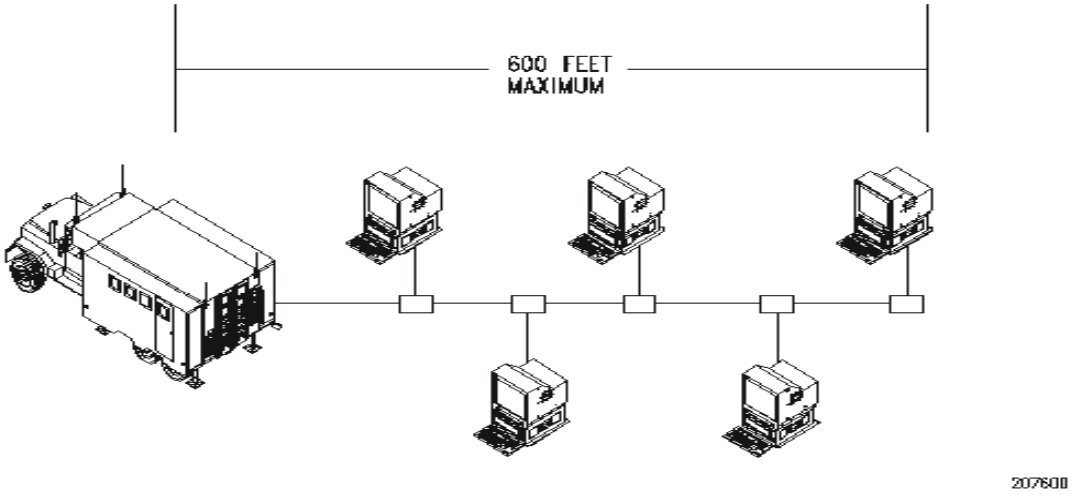

Figure A-2. Generic Tactical LAN Configuration

A tactical LAN is configured to interconnect various TOC shelters. The LAN manager is usually the deputy G6 and or S6. The corps and division deputy G6 and the brigade and battalion S6 have approval authority over all systems connected to their LAN. They ensure the LAN is connected to the WAN. See FM 24-7 for additional information.

WAN

Data and signal distribution between computer systems covering a large geographic area is accomplished by a WAN. LANs or computers connected to telephone lines, radios, or satellite links form a WAN. Figure A-3 shows several widely spread sites connected in a WAN. WANs are also valuable when some of the sites are on the move and relocate frequently. WANs require devices such as modulators/demodulators, multiplexers, or front-end processors to convert the computer data into a form, which can be transmitted over wires or radio links. In addition they must have communications software to control the transmission and reception of the data.

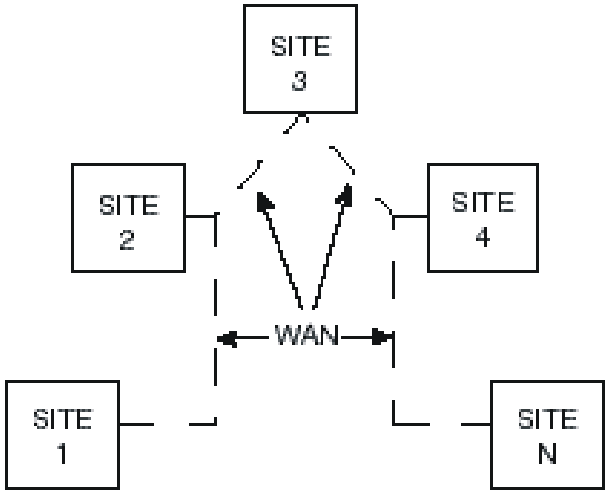

Figure A-3. WAN Connectivity

Digital command posts are normally connected on a WAN. The WAN consists of three types of networks:

- MSE network.
- Global Broadcast Service (GBS).
- Near-Term Data Radio (NTDR).

The LAN connects to the WAN at a gateway. The gateway is located in a SEN or LEN. The G6/S6 and supporting signal unit is responsible for connectivity to the SEN and WAN operations.

TI

The TI is integrated with ABCS but focused at providing the necessary information exchange for battle command at brigade and below. The FBCB2 devices of the TI are integrated into TOC LANs at battalion and brigade echelons, thus enabling information flow from the soldier/platform level to the division and throughout ABCS. EPLRS also links the TI to ABCS at the brigade and battalion TOCs. The EPLRS network provides the primary data and imagery communications transmission system at these echelons.

ROUTER

A tactical LAN consists of several separate LANs interconnected by routers. The tactical LAN interconnects the various TOC shelters. Routing is moving information across an internetwork from the source to the destination. Along the way, at least one intermediate node is encountered. Routing involves two basic activities: determination of optimal routing paths and the transfer of information groups through an internetwork. When a router receives an incoming packet of information, it checks the destination address and attempts to associate this address with the next hop (router).

SWITCHES

A LAN switch is a device that typically connects LAN segments and a high-speed port. A LAN switch has a dedicated bandwidth per port. When a LAN switch is powered up and the devices that are connected to it request services from other devices, the switch builds a table that associates addresses of each local device with the port number through which that device is reachable. See FM 24-7 for a more detailed discussion on router and switch-based TOC architecture.

TACTICAL COMMUNICATIONS INTERFACE MODULE (TCIM)

The TCIM provides Ethernet LAN-based hosts with access to the WAN for FS ABCS systems.

COMBAT SERVICE SUPPORT AUTOMATED INFORMATION SYSTEM INTERFACE-ENHANCED (CAISI-E)

The CAISI-E is a device that provides tactical network connectivity for the logistics community STAMIS. It provides packet connectivity to the TPN, allows systems using asynchronous serial protocols to communicate over Transmission Control Protocol/Internet Protocol (TCP/IP) networks, and serves as a concentrator by allowing multiple users to effectively utilize the limited access ports to the MSE TPN. The CAISI-E serves as an X router, which provides network address translation (NAT) service, Dynamic Host Configuration Protocol (DHCP), and private network for up to 252 IP addresses hidden behind a single registered IP address on the TPN/Non-secure Internet Protocol Routing Network (NIPRNET).

System Security

Information assurance investigates security vulnerabilities in distributed information systems and develops architectures, systems, and techniques for providing protection from attack and exploitation. This appendix covers the procedures for the security and protection of systems that create, process, store, and transmit sensitive but unclassified (SBU), classified, and caveated/handling coded information.

OVERVIEW

If the MAU discovers or suspects a virus or security violation, they should first notify their local terminal area security officer (TASO). The TASO will investigate the problem and determine if it can be corrected locally or if notification of the information system security officer (ISSO) is required. If it is determined that the problem must be reported, the TASO will contact the ISSO located in the support S6. The TASO will identify the security violation or virus information, system identification, and hardware information.

Units have the ultimate responsibility to maintain information systems security (ISS) of their automated systems. Automated systems that have classified or SBU data and require external maintenance support must have data removed before the system is turned over to maintenance support. If the data is not accessible because of a faulty drive reader or some other fault, the data on the system must be cleared, purged, declassified, or destroyed before the system is turned over to maintenance support.

SECURITY PROCEDURES

The information systems security manager (ISSM) is responsible for the security of all information systems and media assigned to the organization and under his purview. To protect these assets, he must ensure that the security measures and policies contained within this appendix are followed. Additionally, the ISSM will publish supplemental organizational procedures (standing operating procedures (SOPs), and so forth), if needed, to implement the requirements herein.

The procedures contained below meet the minimum-security requirements for the clearing, declassifying, degaussing, destruction, storage, sanitizing, and overwriting of magnetic media. These procedures will be followed when it becomes necessary to release magnetic media, regardless of classification, from sensitive compartmented information (SCI) channels.

Overwriting cannot sanitize media that has contained SCI, other intelligence information, or restricted data; such media must be degaussed before release. Media that never contained cryptographic (CRYPTO) material cannot be sanitized at all; such media must be destroyed.

CLEARING MEDIA

Clearing media is erasing or overwriting all information on the media without the totality and finality of purging. The clearing procedure is adequate when the media will remain within a certified facility (vault, room, and so forth); however, removable media that is not

cleared must continue to be controlled at its prior classification or sensitivity level. Purging or sanitizing of media means to erase or overwrite, totally and unequivocally, all information stored on the media.

DECLASSIFYING MEDIA

Declassifying media is the administrative action taken after it is purged. Declassifying is required when the media must leave the facility under the control of uncleared personnel; that is for maintenance operations.

Media can be declassified only after purging. The appropriate ISSO must verify that the technique chosen for purging (or sanitizing) meets applicable requirements. The ISSO must establish a method to periodically verify the results of the purging. As a minimum, a random sampling will be taken to verify each purge.

Transporting media

Transporting any media, such as hardware/items, that could not be declassified or purged will require personnel with the same level of clearance or higher as the hardware/items being transported. This is in accordance with AR 25-IA.

DEGAUSSING

Degaussing (that is demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitation process. Degaussing is more effective than overwriting magnetic media.

Magnetic media is divided into three types (I, II, and III) based on its coercively. Coercively of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercively must be ascertained prior to executing any degaussing procedure. The individual performing the physical degaussing of a component must ensure that the degausser can meet or exceed the coercively factor of the media and that the proper type of degausser is used for the material being degaussed. The three types of degaussers are—

- Type I, which is used to degauss Type I media (that is media for which coercively is no greater than 350 oersteds (Oe)).
- Type II, which is used to degauss Type II media (that is media for which coercively is no greater than 750 Oe).
- Type III, which is used to degauss Type III media (that is media for which coercively is in excess of 750 Oe). Currently there are no degaussers that can effectively degauss all Type III media. Some degaussers are rated above 750 Oe, and their specific approved rating will be determined prior to use.

Refer to the current issue of the National Security Agency (NSA) Information Systems Security Products and Services Catalogue (Degausser Products List Section) for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specification. National specifications provide a test procedure to verify continued compliance with the specification.

Once a degausser is purchased and becomes operational, the gaining organization must establish a SOP explaining how it will be used. Tables A-1 and A-2 provide instructions for sanitizing data storage media and system components. Data storage media will be destroyed in accordance with the designated approval authority/service certifying organization (DAA/SCO) approved methods.

MEDIA DESTRUCTION

Magnetic storage media that malfunctions or contain features that inhibit overwriting or degaussing will be reported to the ISSO. The ISSO will coordinate the repair or destruction of the media with the ISSM and responsible DAA/SCO.

Destroying is the process of physically damaging the media to the level that the media is not usable as media and there is no known method of retrieving the data. Army Regulation (AR) 380-5 governs the destruction of most AIS media. AR 380-19 and Director of Central Intelligence Directive (DCID) 1/21 provides guidance on the destruction of laser printer cartridges.

Destruction of Expendable Items

Destruction of expendable items (for example, floppy diskettes) is not authorized for release to outside of the SCI community. If these items are damaged or no longer deemed usable, they will be destroyed. When destroying, remove the media (magnetic Mylar, film, ribbons, and so forth) from any outside container (reels, casings, hard or soft cases, envelopes, and so forth) and dispose of the outside container in a regular trash receptacle. Cut the media into pieces (a crosscut chipper/shredder may be used to cut the media into pieces) and then burn all pieces in a secure burn facility. If applicable, environmental laws do not permit burning of a particular magnetic recording item; it will be degaussed, cut into pieces (a chipper/shredder preferred), and disposed of in a regular trash receptacle.

Table A-1. Sanitizing Data Storage Media

Media Type	Procedure(s)
Magnetic tape	
Type I	a or b
Type II	b
Type III	Destroy
Magnetic disk packs	
Type I	a or b
Type II	b
Type III	Destroy
Magnetic disks	
Floppies	Destroy
Bernoulli	Destroy
Removable hard disks	a or b or c
Nonremovable hard disks	a or b or c
Optical disks	
Read Only (including CD ROMs)	Destroy
Write Once, Read Many (WORM)	Destroy
Read Many, Write Many	Destroy

Procedures:

a. Degauss with a Type I degausser.

b. Degauss with a Type II degausser.

c. Overwrite all locations three times (first time with a random character, second time with a specified character, and third time with the complement of the specified character).

Note: The ISSO will perform or supervise these procedures.

Table 2. Sanitizing System Components

Type of Component	Procedure(s)
Magnetic bubble memory	a or b or c
Magnetic core memory	a or b or d
Magnetic plated wire	d or e
Magnetic-resistive memory	Destroy
Solid state memory components	
Dynamic random access memory (DRAM) (Volatile)	Destroy
If RAM is functioning	d, then e and i
If Ram is defective	f, then e and i
Static random access memory (SRAM)	j
Programmable ROM (PROM)	Destroy (see h)
Erasable programmable ROM (EPROM/UVPROM)	g, then c and i
Electronically erasable PROM (EEPROM)	d, then i
Flash EPROM (FEPROM)	d, then i

Procedures:

a. Degauss with a Type I degausser.

b. Degauss with a Type II degausser.

c. Overwrite all locations with a random character, a specified character, and then its components.

d. Overwrite all locations with a random character, a specified character, and then its components.

e. Remove all power, including batteries and capacitor power supplies from RAM circuit board.

f. Perform three power on/off cycles (60 seconds on, 60 seconds off each cycle, at a minimum).

g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time | |requirements by a factor of 3.

h. Destruction required only if ROM contained a classified algorithm or classified data.

i. Check with the DAA/SCO to see if additional procedures are required.

j. Store a random unclassified test pattern for a time period comparable to the normal usage cycle.

Note: The ISSO will perform or supervise these procedures.

Destruction of Removable Hard Disks and Disk Packs

Removable hard disks are expendable items and are not authorized for release outside of the SCI community unless they have been degaussed and declassified. Each item is considered classified to the highest level of data stored or processed on the information system in which it was used. If removable hard disks are damaged or no longer deemed usable, they are destroyed. If the platter(s) of the defective unit can be removed and the removal is cost effective, then destruction of a removable hard disk consists of dismantling the exterior case and removing the platter from the case. Local destruction of the platter consists of removing the magnetic surface by sanding.

Disk packs are considered classified to the highest level of data stored or processed on the information system in which it was used. If disk packs are damaged or no longer deemed usable, they are destroyed. Local destruction of the platter consists of removing the magnetic surface by sanding.

STORAGE MEDIA

Storage media containing SCI will be handled as stated in AR 380-19.

OVERWRITING

Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing. However, the effectiveness of the overwrite procedure may be reduced by several factors, including ineffectiveness of the overwrite procedures, equipment failure (for example, misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps.

The preferred method to clear magnetic disks is to overwrite all locations three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character). The overwrite procedure must be verified by the ISSM or designee.

SANITIZING

Sanitizing is the process of removing the data on the media before the media is reused in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing. In general, laboratory techniques cannot retrieve data that was sanitized/purged. Sanitizing may be accomplished by degaussing.

The following procedures are used to clear and sanitize magnetic storage media that is no longer useable, requires transfer, or should be released from control. Personnel needing to destroy, degauss, overwrite, declassify, downgrade, release, or ship media from AISs for all classification levels (to include COMSEC keying material) must follow the rules and Table A-1. If an item is not contained in Table A-1, the headquarters level information systems security program manager (ISSPM) must be contacted for directions.

MEMORY COMPONENTS AND BOARDS

Prior to the release of any malfunctioning memory components and boards, the following requirements will be met in respect to coordination, documentation, and written approval. This section applies only to components identified by the vendor or other technically knowledgeable individual that can retain user-addressable data. It does not apply to other items (for example, cabinets, covers, or electrical components not associated with data), which may be released without reservation. For the purposes of this section, a memory component is considered to be the lowest replacement unit in a hardware device. Memory components reside on boards, modules, and subassemblies. A board can be a module or may consist of several modules and subassemblies. Unlike magnetic media sanitation, clearing may be an acceptable method of sanitizing components for release (see Table A-2). Memory components are specifically handled as either volatile or nonvolatile.

VOLATILE MEMORY COMPONENTS

Volatile memory components do not retain data after removal of all electrical power sources; and when reinserted into a similarly configured system, do not contain residual data. Volatile memory components that have contained extremely sensitive or classified information may be released only in accordance with procedures developed by the ISSM or designee and stated in the accreditation support documentation. A record must be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.

NONVOLATILE MEMORY COMPONENTS

Nonvolatile memory components that do retain data when all power sources are discontinued are ROM, programmable ROM (PROM), or erasable PROM (EPROM), and their variants that have been programmed at the vendor's commercial manufacturing facility and are considered to be unalterable in the field may be released. All other nonvolatile components (for example, removable/nonremovable hard disks) may be released after successful completion of the procedures outlined in Table B-2. Failure to accomplish these procedures will require the ISSM, or designee, to coordinate with the DAA/SCO to determine releasability.

Visual Displays

.A visual display is considered sanitized if no sensitive information is etched into the visual display phosphor. The ISSO should inspect the face of the visual display without power applied. If sensitive information is visible, destroy the visual display before releasing it from control. If nothing is visible, the ISSO shall apply power to the visual display; then vary the intensity from low to high. If sensitive information is visible on any part of the visual display face, the visual display is destroyed before it is released from control.

Printer Platens and Ribbons

Printer platens and ribbons are removed from all printers before the equipment is released. One-time ribbons and inked ribbons are destroyed as sensitive material. Wiping the surface with alcohol shall sanitize the rubber surface of platens.

Laser Printer Drums, Belts, and Cartridges

Laser printer components containing light-sensitive elements (for example, drums, belts, complete cartridges) are sanitized before release from control.

Elements containing information that is classified, but is not intelligence information, can be considered sanitized after printing three printer-font test pages.

Elements containing intelligence information are sanitized in accordance with the policy contained in DCID 1/21.

RELEASE OF SYSTEMS AND COMPONENTS

The ISSM, or designee, shall develop equipment removal procedures for systems and components and these procedures are stated in the accreditation support documentation. When such equipment is no longer needed, it can be released if—

- The ISSM, or designee, inspects it. This inspection will assure that all media, including internal disks, have been removed or sanitized.
- A record is created of the equipment release indicating the procedure used for sanitation and to whom the equipment was released. The record of release is retained for a period prescribed by the DAA/SCO.
- Procedures specified by the DAA/SCO are used.

Following release, administratively notify the DAA/SCO. The NSA/Central Security Service (CSS) Form G6522 or similar form or documentation will be used to document the local release or disposal of any information system or component.

Refer to AR 380-19, AR 25-IA, and AR 380-5 for procedures on information assurance.

Glossary

A2C2	Army Airspace Command and Control
ABCS	Army Battle Command System
ACUS	Area Common User System
ADA	Air Defense Artillery
ADDS	Army Data Distribution System
ADPE	automated data processing equipment
AFATDS	Advanced Field Artillery Tactical Data System
AIS	automated information system
AIT	automated information technology
AMC	Army Materiel Command/Area Maintenance Company
AMD	Air and Missile Defense
AMDPCS	Air and Missile Defense Planning and Control System
AMSS	Army Materiel Status System
AO	Automation Officer
AOE	Army of Excellence
AR	Army regulation
ASAS-RWS	All Source Analysis System-Remote Workstation
ASG	area support group
ASL	authorized stockage list
BCT	brigade combat team
BFA	battlefield functional area
BSA	brigade support area
BSC	base support company
C2	command and control
CAISI	Combat Service Support Automated Information System Interface
CAISI-E	Combat Service Support Automated Information System Interface-Enhanced
CASCOM	U.S. Army Combined Arms Support Command
CECOM	Communications-Electronics Command
CD-ROM	compact disk-read only memory
CHS	common hardware/software
COMSEC	communications security

CONUS	continental United States
CofS	Chief of Staff
COSCOM	Corps Support Command
COTS	commercial-off-the-shelf
CRT	combat repair team
CSB	corps support battalion
CSG	corps support group
CSS	combat service support
CSSAMO	Combat Service Support Automation Management Office
CSSCS	Combat Service Support Control System
CSLA	Communications Security Logistics Activity
CTA	common table of allowances
CTSF	Central Technical Support Facility
DAA/SCO	designated approval authority/service certifying organization
DAMMS-R	Department of the Army Movement Management System-Redesign
DASB	division aviation support battalion
DBMS	Database Management System
DC	District of Columbia
DCID	Director of Central Intelligence Directive
DDN	Defense Data Network
DISCOM	Division Support Command
DISN	Defense Information System Network
DIVARTY	division artillery
DMS	Defense Messaging System
DS	direct support
DSA	division support area
DSB	division support battalion
DTSS	Digital Topographic Support System
EAC	echelons above corps
EAD	echelons above division
ECB	echelons corps and below
ESSC	Electronic Sustainment Support Center
ETM	electronic technical manual
EW	electronic warfare
FA	functional area/field artillery
FAADC3I	Forward Area Air Defense Command, Control, Computer, and

	Intelligence System
FBCB2	Force XXI Battle Command-Brigade and Below
FDD	first digitized division
FRA	forward repair activity
FS	fire support
FSB	forward support battalion
FSC	forward support company
FSCOORD	fire support coordinator
G4	Assistant Chief of Staff, G4 (Logistics)
G6	Assistant Chief of Staff for Information Management-G6
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System–Army
GCSS-A	Global Combat Support System-Army
GMC	ground maintenance company
GOTS	government-off-the-shelf
GS	general support
GTE	General Telephone and Electronics
HCLOS	high-capacity line-of-sight
HSC	headquarters and supply company
IA	information assurance
IEW	intelligence and electronic warfare
IMETS	Integrated Meteorological System
IMO	information management officer
INE	inline network encryption
INFOSEC	information security
IP	Internet Protocol
ISS	information system security
ISSM	information system security manager
ISSO	information system security officer
ISYSCON	integrated systems control
JCDB	joint common database
LAN	local area network
LAR	logistics assistance representative
LEN	large extension node
LOGSA	logistics support activity

LOS	line-of-sight
LRU	line replaceable unit
LSE	logistic support element
MAA	mission application administrator
MACOM	major Army command
MAU	mission applications user
MCS	Maneuver Control System
METT-TC	mission, enemy, terrain, troops, time and civilian considerations
MI	military intelligence
MLRS	Multiple Launch Rocket System
MODEM	modulator/demodulator
MOS	military occupational specialty
MP	military police
MSB	main support battalion
MSE	mobile subscriber equipment
MST	maintenance support team
NC	node center
NDI	nondevelopmental items
NSA	National Security Agency
NTDR	Near Term Data Radio
OSC	objective supply capability
PC	personal computer
PEO	Program Executive Office
PMO	Project/Product/Program Management/Manager Office
PMCS	preventive maintenance checks and services
QM	quartermaster
RSC	Regional Support Center
S2	Intelligence Officer (Army)
S3	Operations and Training Officer (Army)
S4	Supply Officer (Army)
S6	Communications Staff Officer
SAAS-MOD	Standard Army Ammunition System-Modernization
SAMS	Standard Army Maintenance System
SARSS	Standard Army Retail Supply System
SCI	sensitive compartmented information
SCX	STAMIS Computer Exchange

SDS	Standard Depot System
SEN	small extension node
SINCGARS	Single-Channel Ground and Airborne Radio System
SINCGARS-ASIP	Single-Channel Ground and Airborne Radio System-Advanced System Improvement Plan
SICPS	Standardized Integrated Command Post System
SIDPERS	Standard Installation/Division Personnel System
SNMP	Simple Network Management Protocol
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SPBS-R	Standard Property Book System-Redesign
SRU	shop replaceable unit
SMART-T	Secure Mobile Antijam Reliable Terminal-Tactical
SSA	supply support activity
ST	Special Text
S&T	supply and transportation
STAMIS	Standard Army Management Information System
TACSAT	tactical satellite
TAIS	Tactical Airspace Information System
TASO	terminal area security officer
TAMMIS	The Army Medical Management Information System
TCAIMS-II	Transportation Coordinator Automated Information for Movements System-II
TCIM	Tactical Communications Interface Module
TCP/IP	Transmission Control Protocol/Internet Protocol
TDA	tables of distribution and allowances
TFSA	task force support area
TI	Tactical Internet
TMDE	test, measurement, and diagnostic equipment
TOC	tactical operations center
TOE	table(s) of organization and equipment
TP	Transfer Protocol
TPN	Tactical Packet Network
TRADOC	Training and Doctrine Command
TSC	Theater Signal Command
TYAD	Tobyhanna Army Depot
ULLS-A	Unit Level Logistics System- Aviation

ULLS-G Unit Level Logistics System-Ground

ULLS-S4 Unit Level Logistics System-S4

U.S. United States

VIC3 vehicle internal command, control and communications

XO Executive Officer

WAN wide area network

WIN Warfighter Information Network

WIN-T Warfighter Information Network-Tactical